#WatchOut

Analysis of smartwatches for children

October, 2017

FORBRUKERRÅDET

Content

Summary

As a part of our work on the Internet of things, the Norwegian Consumer Council (NCC) has analyzed consumer rights in four smartwatches for children. These devices were all bought in Norwegian stores, and are called Gator 2, Tinitell, Viksfjord, and Xplora. These smartwatches for children are wearable mobile phones that allow parents to use an app on their smartphones to keep in touch with and track the location of their children. Since the main purpose of these devices is to give parents peace of mind while their children play freely outside, we see it as crucial that they maintain adequate security and privacy standards.

The project consists of two parts: an analysis of the features of the apps/devices and the accompanying user terms, presented in the WatchOut report, and a technical report commissioned by the NCC and produced by the IT security company Mnemonic.

Devices that use the Internet to allow real-time location tracking of, and direct communication with, young children, and which store names, photos and continuous and historic geolocation data, should have strong safeguards in place. This entails not only a high level of security to avoid unwanted access, but also a robust framework to ensure that data protection laws and the privacy rights of children are respected and upheld. Three out of the four watches that were analyzed fall short in both respects.

Critical security flaws

The tests done by Mnemonic have uncovered critical security flaws in three of the apps and devices. As detailed in Mnemonic´s report, two of the devices have flaws which could allow a potential attacker to take control of the apps, thus gaining access to children's real-time and historical location and personal details, as well as even enabling them to contact the children directly, all without the parents' knowledge. Additionally, several of the devices transmit personal data to servers located in North America and East Asia, in some cases without any encryption in place. One of the watches also functions as a listening device, allowing the parent or a stranger with some technical knowledge to audio monitor the surroundings of the child without any clear indication on the physical watch that this is taking place.

A false sense of security

We have also found that the advertised safety-enhancing features, such as an SOS button that alerts the parents if the child is in distress, and a geofencing function that sends an alert whenever the child enters or leaves a designated area, were unreliable. In practice, this means that the device might in fact provide a false sense of security. This is especially disconcerting since the smartwatches are meant to provide peace of mind for the parents who purchase the devices.

Lack of respect for consumer rights

Inadequate and unclear user terms deny consumers their basic consumer and privacy rights when engaging with these products. Only one of the services actually asks for consent to data collection, none of them promise to notify users of any changes to their terms, and there is no way to delete user accounts from any of the services. At least one of the companion (Xplora) apps also allows children's personal data to be used for marketing purposes, while the other three are unclear about how this information may or may not be used. Additionally, one of the services (Gator) transmits unencrypted children's location data to China. Together, these issues constitute several breaches of European data protection and consumer protection laws.

Chaotic market

Additionally, the abundance of smartwatches for children available internationally, with cheap Chinese products being imported and rebranded by a vast number of local retailers, makes it difficult to obtain a clear picture of who is responsible for the various products. For example, several different smartwatches for children use the same app as the Viksfjord watch, the SeTracker app. Some of these devices are seemingly identical to Viksfjord, but are sold under different names on a worldwide basis. As far as we can tell, all the watches using the SeTracker app have the same security and privacy vulnerabilities as the Viksfjord.

Overall, we have uncovered many serious problems with smartwatches for children. It seems clear that consumers currently should think twice before purchasing these or similar devices.

The findings also serve to illustrate the emerging problems facing consumers in the world of connected devices, and the need to make sure that product safety regulations also apply to products with digital components.

Summary of terms

	 Gator	 Tinitell	 Viksfjord/ SeTracker	 Xplora
Consent is sought at registration.	✗	✓	✗	✗
I will be notified if the terms are changed.	✗	✗	✗	✗
My personal data will not be used for marketing purposes.	✗	?	?	✗
I can delete data in the app.	✗	✗	?	?
Location data is automatically deleted after a set period of time.	✗	✗	✗	✗
I can delete my user account.	✗	✗	✗	✗
Promises to implement reasonable security standards.	✗	✓	✗	✗
It is made clear where personal data is transmitted and stored.	✗	✗	✗	✗

Analysis of smartwatches for children

In the course of the last 10 years, smartphones have become ubiquitous in Norway, resulting in the vast majority of the population carrying small Internet-connected computers around with them wherever they go. In addition to pocket-sized devices, wearable computers have also become popular, for example through the Apple Watch or fitness trackers.[1] For parents of young children, the desire to keep in touch with their children may have come into conflict with the view that the child is too young to have an expensive and complicated smartphone. This could explain the rising popularity of smartwatches for children, which facilitate easy communication without the worry of children losing their phones.

Smartwatches for children contain a SIM-card, allowing them to connect to the Internet through GSM-networks or through a Wi-Fi connection. In its most basic form, the smartwatch functions as a mobile phone attached to the wrist, which connects to the parents' phones through an app. The features of the devices vary between devices and apps, but all of the smartwatches in our study come with basic GPS functionality, allowing parents to track the movements of their children in real time through a companion mobile app. These apps are connected to the Internet, allowing a variety of other features. The devices have proven quite popular on the Norwegian market, and have received a lot of media attention. As an indication of the technology's rising popularity, the tech research company Gartner predicts that children's smartwatches will account for 30% of smartwatch shipments in 2021.[2]

When mapping the Norwegian and European market for available and popular smartwatches, the Norwegian Consumer Council (NCC) discovered a fragmented and complex market landscape. Many of the devices seem to originate from and/or be produced in China, and are imported to different European markets through specialized websites run by startups or enterprising individuals, in addition to traditional retailers. Distributors in different countries rebranding the devices under different names further complicates the picture. This obscures the fact that the actual devices are often more or less identical to ones that can be ordered from Chinese online marketplaces such as AliBaba and AliExpress. Additionally, some startups claim to have released their own unique versions of the devices, which could be specially tailored for local customers.

As the main selling point of smartwatches for kids seems to be added safety and peace of mind for parents, the NCC were interested in testing the actual safety measures implemented in the devices. The Internet connectivity of the apps also suggests that a variety of data is transmitted online, including exact, real-time location data. Under European data protection regulations, continuous location data, especially when combined with other information such as a

1 https://www.forbrukerradet.no/side/fitness-wristbands-violate-european-law/
2 http://mobilemarketingmagazine.com/310m-global-wearable-sales-2017-gartner

unique identifier, is considered personal data.[3] This means that such information merits special protection under European legislation, and appropriate measures must therefore be taken to protect the privacy of consumers.

The four smartwatches analyzed by the NCC are the Gator 2, Tinitell, Viksfjord, and Xplora. These devices come with different sets of features, but all four are, or claim to be, popular on the Norwegian market. They are available in known Norwegian retailers such as XXL and Enklere Liv, and from international retailers such as Amazon, AliExpress, and Wal-Mart.

Methodology

As a part of our work with mobile apps[4] and connected devices,[5] the NCC has developed a set of criteria used to analyze the features and user agreements of various digital products and services. This method includes user testing the services in question and reading any available relevant legal documents, typically consisting of a privacy policy and terms of use (hereafter collectively referred to as "user terms"). The criteria are based on existing Norwegian and European consumer and data protection regulation, in addition to our own understanding of what consumers should expect when using digital services. The actual services and their terms are then graded on a traffic light-style color scale, where green means that the criteria are fulfilled, red means not sufficiently fulfilled, and yellow means that the results are unclear, or that the subject is not properly addressed or applicable.

The user terms for each individual product are normally provided as a link in the app stores, or in some cases through the service provider's website.[6] They should also be provided when starting the app for the first time, or upon registering a user account. In our analysis of the four devices and services, we discovered that Gator 2 do not provide any user terms or other relevant legal documents for their app. This is cause for concern, as it means that it is impossible for consumers to know their rights when using a Gator product or service. Because of this absence of terms, Gator has received a "red light" on all points related to the content of user terms.[7]

In addition to analyzing user terms, the companion apps were installed, and the watches were tested by following the instructions in the official user manuals. The NCC also commissioned a set of technical tests from the Norwegian cybersecurity company Mnemonic.[8] These technical tests mostly focused on what goes on "under the hood" of the services, looking at data flows and

3 See https://www.datatilsynet.no/regelverk-og-skjema/lover-og-regler/uttalelser-fra-artikkel-29-gruppen/mobilapper-krav/ and http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

4 https://www.forbrukerradet.no/appfail-en/

5 https://www.forbrukerradet.no/internet-of-things/

6 See list at end of document

7 The app Gator 3 supplies a set of terms, but they do not seem to apply to the Gator app. In any case, they are not linked to from the Gator app in the app stores, nor presented upon registration.

8 https://www.mnemonic.no/

analyzing cyber security. Some of the results of these tests are incorporated in this report, with a more complete account included as an attachment.[9]

Features of the devices

Device App	Gator 2 Gator	Tinitell Tinitell	Viksfjord SeTracker	Xplora Xplora T1
Make/receive calls	✓	✓	✓	✓
Contact list[10]	✓	✓	✓	✓
GPS tracking in app	✓	✓	✓	✓
Geofencing[11]	✓	No	✓	✓
SOS button[12]	✓	No	✓	✓
Receive SMS	No	No	No	✓
Voicemail	✓	No	✓	No
Monitoring[13]	No	No	✓	No
Alert if device is removed from arm	No	No	✓	No
Prevent child from turning off device	✓	No	✓	No

9 Mnemonic 2017, "Security Assessment of GPS Watches for Children"

10 List of numbers that the device can call, and who are allowed to call the device.

11 A defined geographical zone. If the child leaves or enters the area, the parent device receives an alert.

12 Button that automatically calls a pre-defined number.

13 Function that allows the parent to listen in on the smartwatch, without the child knowing.

Gator 2

The Gator 2 watch is produced by the Chinese company Gator Group, and is distributed in Norway by the company Gator Norge.[14] Gator is also marketed in some countries under the brand Caref.[15] The watch requires a SIM card in order to work, which has to be bought separately from a service provider of the user's choice. The companion app, also called Gator, contains several functions beyond simple GPS tracking, including geo-fencing ("safe zones"), voicemail, and a step counter.[16] There is also an SOS button, which immediately makes a call to the parent's device. However, during the testing done by both the NCC and Mnemonic, this function was found to be unreliable. At times the SOS button only worked once, and the device had to be restarted to enable the function again. On other occasions, the button did not work at all. [17]

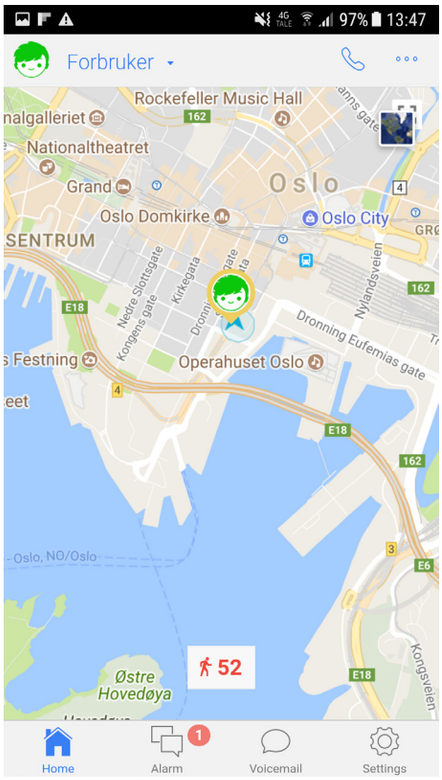


Photo: The Gator app

The device itself has a colored LED screen, and instead of having a touch screen it is controlled through a combination of button presses. On its website, Gator claims to be the most sold smartwatch for children in Norway, and boasts of 300 000 units sold worldwide.[18] The test model was purchased in the major Norwegian sporting goods store XXL.[19] In September 2017, the new model Gator 3 was released in Norway. GatorNorge has in parallel launched the app TeleGApp which, as far as we understand, will in time become the companion app for the Gator 3, but at the time of launch, the Gator 3 watch is paired with the Gator 3 app .[20]

14 https://www.gatornorge.no/

15 The Caref watch sold in the US uses a different app than the Gator2 http://carefgps.com/index.html

16 https://play.google.com/store/apps/details?id=com.gatorgroup.carefwatch

17 Mnemonic 2017, "Security Assessment of GPS Watches for Children"

18 https://www.gatornorge.no/

19 https://xxl.no/gator-mobile-watch-gator-2-gps-klokke-med-telefon/p/1132552_2_style

20 The app that replaces the Gator app is called TeleGApp, and comes with user terms that allow personal data to be sold.

Tinitell

The smartwatch Tinitell was originally financed through the crowdfunding site Kickstarter, and has since branched out from Tinitell's native Sweden.[21] Although Tinitell does not seem to have any direct relationship with any telephone company, a SIM card from Telenor was included with the purchase. The device can also be used with SIM cards from other providers. As the product moves into the American market, Tinitell is also set to be integrated with Amazon's voice assistant Alexa.[22] With no screen on the device, and with a companion app that only tracks location and allows phone calls to the watch,[23] Tinitell is the most "stripped down" product that was analyzed. The NCC has not been able to find concrete sales numbers for Tinitell, but in 2015 the CEO claimed to have sold 40 000 devices.[24] The device was purchased from the electronics retailer Kjell & Company.[25]

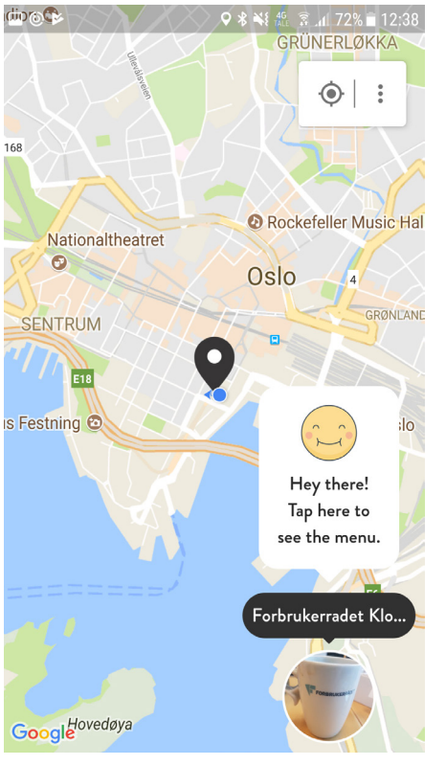


Photo: Tinitell app

Viksfjord/ the SeTracker family of smart watches

The Viksfjord watch is distributed in Norway through the website GPS for Barn ("GPS for Kids"), which sells three different smartwatch models.[26] Although the brand name Viksfjord seems to be uniquely Norwegian, more or less identical versions of the device are sold all over the world bearing countless different brand names, and it can also be purchased in Norway under the name Spectrafence.[27] The watch we tested had the name Viksfjord printed on the

21 http://tinitell.com/kickstarter/

22 https://venturebeat.com/2017/07/17/amazons-alexa-accelerator-announces-its-first-13-week-startup-class/

23 https://play.google.com/store/apps/details?id=com.tinitell.tguardian

24 http://www.adweek.com/digital/sxsw-marketers-smartphone-apps-are-yesterdays-news-wearables-are-what-matter-163483/

25 http://www.infomark.co.kr/en/bbs/board.php?bo_table=menu01&wr_id=61

26 http://gpsforbarn.no/

27 https://www.jollyroom.no/barneklaer/tilbehor/barneklokker/spectrafence-gps-klokke-rosa

front, but this label rubbed off after 30 minutes of use. Viksfjord uses the companion app SeTracker.

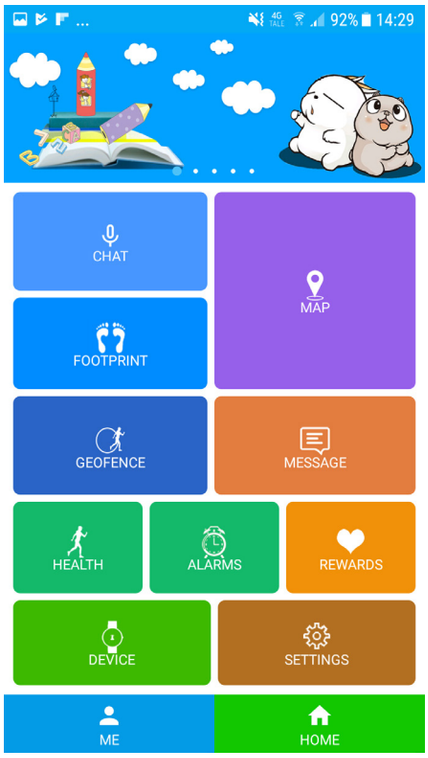


Photo: Viksfjord app

Because of the large variety of distributors and brands connected to the SeTracker family of devices, the original manufacturer of the device is somewhat unclear. As far as the NCC have been able to ascertain, the Chinese companies 3G Electronics[28] and Wonlex are likely originators.[29] In the device purchased by the NCC, a SIM card from the telephone company TalkMore was included. It turned out that activating this SIM card would begin a subscription for NOK 99 per month. However, the watch also functions with SIM cards from other providers.

On GPS for Barn's Facebook page, they claim 500 000 units sold worldwide.[30] The device is operated by swiping on a touchscreen, in addition to an SOS button. In addition to smartwatches for children, the Viksfjord watch (or a near-identical product) is also available as a tool for dementia patients.[31] Both the dementia patient version and children's version of the device are listed on the Norwegian Labour and Welfare Administration's database for health and welfare-related tools.[32] The test version of the Viksfjord was bought at the Norwegian lifestyle shop Enklere Liv.[33]

The companion app, called SeTracker,[34] is similarly available to consumers all over the world, boasting more than 4 200 000 total downloads.[35] This app is the most feature-rich service that the NCC looked at, with functions including fitness tracking, a "reward" system, a "friend" system, geofencing, "monitoring"[36], and more. However, the poor translation in the app makes it difficult to understand what many of the functions actually do. SeTracker is the companion app for a wide range of different smartwatches, which are also sold all over the

28 http://en.3g-elec.com/

29 http://www.iwonlex.com/products/wonlex-waterproof-kids-gps-watch-gw100s/

30 https://www.facebook.com/gpsforbarn/photos/a.579363402219223.1073741828.564882490333981/842597885895772/?type=3&theater

31 https://gpsfordemente.no/

32 http://www.hjelpemiddeldatabasen.no/r11x.asp?linkinfo=48994

33 https://www.enklereliv.no/gpsforbarn.html

34 https://play.google.com/store/apps/details?id=org.zywx.wbpalmstar.widgetone.uexaaagg10003

35 http://www.iwonlex.com/kids-gps-watch-solution/

36 The "monitor" function allows the user of the app to send an SMS to the watch, which makes the watch place a covert call to the parent phone. This results in a one-way conversation, where the parent can listen in on the child (and their surroundings) without the child being aware of this happening.

world under different names.[37] The functions provided in the app vary somewhat between devices, and the physical product may be produced by different companies for all we know, but the app is the same across the whole spectrum of watches.

Xplora

Xplora is distributed by the Norwegian telephone company PepCall, and is only sold with a SIM card with a non-cancellable 12-month subscription to PepCall's services.[38] On Xplora's website, they state that the device will not work with SIM cards from other providers, even after the initial 12-month subscription period has ended. Upon inserting a SIM card from another provider, the device returns a "SIM not supported" error.

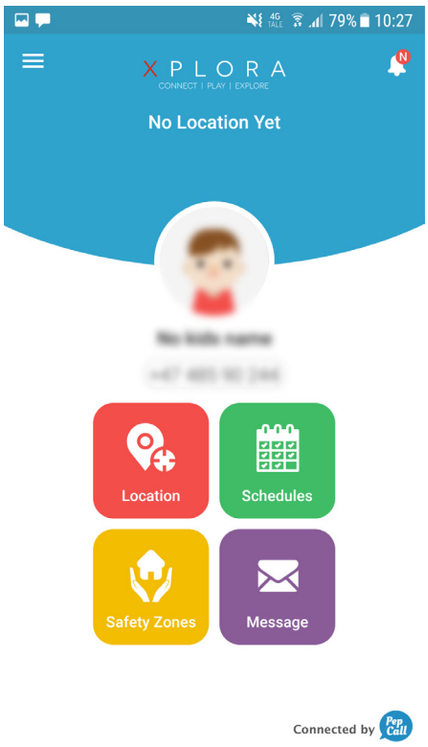


Photo: Xplora app

The actual device is a re-branded version of the smartwatch JOON2, which is produced by the South Korean company Infomark, who are also listed as the developers of the companion app Xplora T1.[39] Xplora claims to have sold 350 000 devices worldwide, and is also available in the UK[40] and Sweden.[41] The watch has also been featured on major Norwegian TV shows, illustrating the popularity of the product.[42] Like Viksfjord, Xplora is also equipped with a touchscreen, and comes with several other functions such as geofencing, SMS, and an SOS button.[43] Xplora is the only one of the four watches where the GPS function is set to not automatically send location updates to the parent's device by default. In order to enable the automatic GPS function, the parent has to make an active choice to switch it on. The NCC purchased the Xplora device from the Norwegian electronics chain Spaceworld Soundgarden.[44]

37 A number of these devices can be found on the Wonlex website. The NCC has found identical devices being sold under different names all across Europe, North America, and Asia. http://www.iwonlex.com/whole-products/gps-tracking-watches/

38 https://xplora.no/xplora/

39 http://www.infomark.co.kr/en/bbs/board.php?bo_table=menu01&wr_id=61

40 http://myxplora.co.uk/

41 http://xplora.se/

42 http://www.tv2.no/v/1065708/

43 https://play.google.com/store/apps/details?id=kr.co.infomark.kidzon.pcbeta&hl=NO

44 https://swsg.no/xplora-mobilklokke-oransje-bla

Functional security

Since the smartwatches make it possible to directly contact children and track their location, the four devices and apps have different safeguards in place to prevent unwanted access.

The Gator watch comes with an IMEI code (unique device identifier) printed on the back, which needs to be scanned or manually entered when connecting to the app. In order to make calls to the watch, phone numbers need to be whitelisted in the app (added to a list of "accepted" numbers), which is meant to prevent strangers from contacting the child. Additionally, if a second parent or guardian wants to connect their phone to the watch, they need a four-digit verification code from the original account, and this code seems to change at a certain interval. However, as noted in the technical report, Mnemonic discovered that some of these security measures were either lacking or poorly implemented.[45]

To connect the Tinitell watch to the companion app, the parent's phone needs to be paired through a short-range Bluetooth connection. The app has an optional function to block numbers that have not been whitelisted. Only one account can be connected to a watch, which gives additional security, but also limits the usability of the device somewhat.

When connecting the Viksfjord device to a phone, one has to scan or enter an IMEI code from the back of the watch, similarly to the Gator unit. Like the Tinitell, the Viksfjord can only be connected to one account at a time. If a new user connects to the watch, the original account seems to be disconnected from the device. As Mnemonic observed in their technical tests, each Viksfjord device can only be registered to an account three times before the registration stops working.[46] The app has a whitelist function, but surprisingly the watch will still accept any calls that hide their caller ID. In practice, this means that anyone who chooses to hide his or her number could directly contact the wearer of the watch. Although this seems like a serious security oversight, the flaw is mentioned in the user manual for the watch, but the manual is not actually included with the product. The document is available through the website GPS for Barn.[47]

The Xplora watch registration process includes sending an SMS code to the phone, which must be entered in the app in order to proceed. To pair the watch with the app, a four-digit code is generated on the watch interface, which also has to be entered in the app. The app can be protected with a PIN code for added security, and includes an option to block numbers that have not been whitelisted. Xplora supports up to five registered accounts simultaneously.

45 Mnemonic 2017, "Security Assessment of GPS Watches for Children"

46 Mnemonic 2017, "Security Assessment of GPS Watches for Children"

47 https://gpsforbarn.no/manual/Manual-Viksfjord.pdf

Phone features

In addition to being GPS trackers, all of the four watches function as wearable phones, marketing themselves as a child's first mobile phone. The watches can hold a limited number of preset phone numbers, which are set in the companion apps. These numbers can be cycled through by swiping or clicking buttons on the devices, in order to place calls to regular phones or other watches. The watches have their own unique phone numbers (tied to the SIM card), which can be called by pre-approved numbers that are set up in the companion app.

The Tinitell, Gator, and Viksfjord are normally used with a prepaid subscription, with SIM cards either included in the box or bought separately. This means that the parent chooses a provider and subscription, pays a certain amount upfront, and tops up the balance if necessary. The Xplora is distributed and sold by the Norwegian telephone company PepCall, and is sold with a non-cancellable 12-month subscription to PepCall's services. With the Tinitell and Viksfjord, replacing the SIM card is fairly straightforward, as the user only has to open a hatch to extract and insert the card. In order to insert or remove a SIM card from the Gator device, one has to unscrew the device completely, which exposes the circuitry within the watch. As mentioned, the Xplora does not function with SIM cards from other providers.

Personal data

Under European legislation, personal data is defined as information that can, by itself or in combination with other data, be used to identify an individual. This includes direct identifiers such as full names, but could also include more technical data such as IP addresses and information gathered from cookies. Precise location data is also considered personal data, especially when continuously collected.[48] Studies have shown that four location points are almost always sufficient to correctly identify an individual.[49] Anyone who collects, stores, or processes such data, has to make sure that sufficient measures are in place to ensure the privacy and security of each individual. The GPS-based functionality of these four devices means that continuous location data is transmitted from the watch and the companion apps, together with unique identifiers such as IMEI numbers and phone numbers. Together, this information constitutes personal data, which is collected by the service providers.[50]

Consent

In order to collect and process personal data in accordance with the EU privacy regulation, all data controllers have to obtain the freely given, specific and informed consent of the data subject[51]. This means inter alia that services

48 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

49 https://www.nature.com/articles/srep01376

50 Mnemonic 2017, "Security Assessment of GPS Watches for Children"

51 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

should not use pre-checked boxes, and that user terms should be understandable for consumers. Unfortunately, the latter is often not the case, as many studies have shown that user terms are unreasonably long and complicated.[52] For digital services, this consent is usually acquired at initial startup of the service, or when the user registers a user account in the app. In most cases, the user terms are displayed or linked to, and the user has to click "I have read and accept these terms" in order to proceed. It is no secret that a vast majority of consumers never read these legal documents, but if they are not even at least presented with the opportunity to do so, consent is clearly not given in accordance with European legislation.[53]

Of the four services that the NCC looked at, only Tinitell actually asks for consent at registration. The terms and conditions are linked to when setting up an account, and the user has to click a button stating "I have read and agree to the terms". There is no box to check, nor is there a button for "I do not agree", but the user is required to actively click the button in order to proceed.

As Gator provides no user terms whatsoever, there would be no way for users to give informed consent even if prompted by the app. The terms for both Viksfjord/SeTracker and Xplora are absent from the signing-up process, and users are not asked for consent during registration. We find this worrying in light of the requirements that apply to data controllers. Aside from location data, user e-mails are required

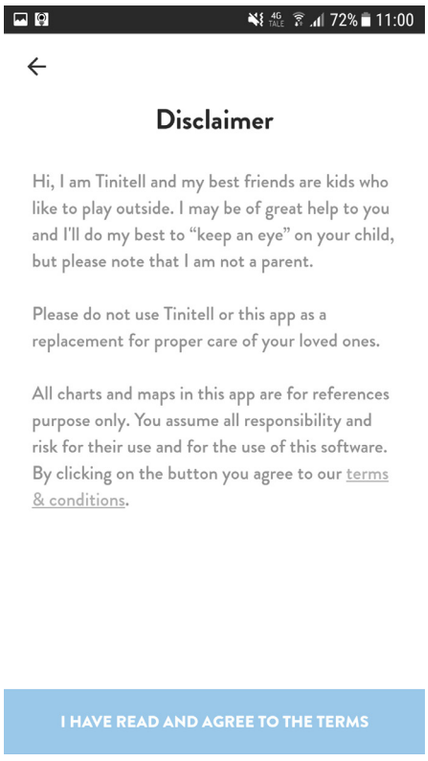


Photo: Disclaimer, Tinitell

52 https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/

53 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

to sign up for an account, which may by itself constitute the collection of personal data. In other words, Gator, Viksfjord/SeTracker, and Xplora all collect at least some personal data about children without valid consent, and thus in breach of European privacy and consumer laws.

Changes in user terms

In addition to having the opportunity to read the user terms upon registration, it is crucial that users are notified if the terms are changed. Even though a user may have consented to the original terms, consent should be sought again if a change alters the user's rights or responsibilities. If changes are made without users' knowledge, the user has no chance to oppose the change, or leave the service if the new terms are unacceptable to them.

> *"If we make any changes to this Privacy Policy, we will change the "Last Updated" date below. We encourage you to review this Privacy Policy whenever you use the Service or visit our Site to understand how your personal information is used."*

Tinitell privacy policy

	Gator	Tinitell	Viksfjord/ SeTracker	Xplora
It is stated when the terms were last changed.	✗	✗	✗	✗
I will be notified if the terms are changed.	✗	✗	✗	✗

Out of the three services that include user terms, none of them promise to notify the users of changes. Both Tinitell and Xplora state that they will notify the users by adding a note in the actual privacy policy, but neither include a "last updated" date in their documents. In addition to simply changing the date in the document being insufficient notice, the failure to include the date makes it effectively impossible for users to tell if any changes have been made. Since the terms for Viksfjord/SeTracker do not state that they will notify users about changes, it is assumed that they will not give such notice. In our opinion, the

failure to notify users could constitute a breach of the Directive on unfair terms in consumer contracts.[54][55]

Purpose limitation

One of the core principles of data protection and privacy legislation is that of purpose limitation, meaning that collected data should not be used for purposes other than the original intent of collection.[56] The "original purpose of collection" should be to provide the service to the user, unless they have explicitly consented to other data usage. In smartwatches for children, the purpose of collection should be to let users of the app track the wearers of the watch, to provide call functions between the two, and possibly a few other functions. This means that some data such as geolocation has to be collected, but this data should not be used for purposes such as profiling users, or to target advertising (without separate and explicit consent).

In their privacy policy, Tinitell state that they:

> *"may use personal information collected through our Site, our Mobile Apps, and Device for the purposes described in our privacy policy or elsewhere on our Site."*
>
> Tinitell privacy policy

They go on to list a few purposes, such as providing the service, transactions, and to provide maintenance based on analysis. These are all justified purposes, but the caveat of "or elsewhere on our site" makes it difficult to know if there are other purposes mentioned outside of the user terms.

54 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31993L0013

55 This formed the basis for the NCCs complaint on Apple to the Norwegian Consumer Ombudsman: https://www.forbrukerradet.no/wp-content/uploads/2015/10/Complaint-on-Apple-iCloud-to-the-Norwegian-Consumer-Ombudsman.pdf

56 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

The user terms of Viksfjord/SeTracker do not mention anything about how they may use personal data, which makes it difficult to understand what they regard as relevant for providing the service. In the Xplora privacy policy, there is a similar list of purposes, but they add that they may use personal information:

> *"for marketing and advertisement".*

Additionally, they state that they:

> *"may collect the following types of information when we provide our services to you. […] Profile information: SNS registration information (twitter ID or/and Facebook ID), member's status information, personal introduction, and interests"*
>
> Xplora privacy policy.

It is not stated why this information is needed, or how it relates to the operation of the services.

> *"We use your personal information for the purposes set out below. […] To develop new services and to use for marketing and advertisement"*
>
> Xplora privacy policy

As far as the NCC is concerned, the use of personal data for advertising purposes is not consistent with the core purposes of data collection for smartwatches, especially since Xplora never obtains user consent for any data collection. Since the service will mostly collect children's data through the device (location, name, photo, etc.), this also raises questions about whether children's personal data from the watch/app is used for advertising purposes on other platforms.

Deletion

In order to have control of their data, users should be allowed to access and delete all information that services have collected about them.[57] In the case of smartwatches, this would typically mean that it should be possible to delete location history. Furthermore, data has to be deleted not only from the user's device/account, but from the servers of the data controller as well.

57 See Directive 95/46/EC – article 1 cf. article 6 and article 12. See also https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf and http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

	 Gator	 Tinitell	 Viksfjord/ SeTracker	 Xplora
I can delete data in the app.	✕	✕	? *	? **
Location data is automatically deleted after a set period of time.	✕	✕	✕	✕ ***

** Some data, such as name. Not location history.*
*** Some data, such as messages.*
**** Claimed to be after 72 hours, but does not happen in practice.*

As far as the NCC was able to find while testing the services, Gator and Tinitell have no way to delete information. Viksfjord/SeTracker lets users delete the user's real name, but location history is seemingly impossible to delete. Xplora permits deletion of messages, but has no manual deletion of location history. However, the Xplora user manual states that location history will be automatically deleted every 72 hours.[58] The technical tests done by Mnemonic showed that this is not correct, as the logged data remained in the app for the entire testing period and Mnemonic found that they could access user data from years ago on other user's devices.[59]

	 Gator	 Tinitell	 Viksfjord/ SeTracker	 Xplora
I can delete my user account.	✕	✕	✕	✕

If the user wants to leave the service, it is usually not enough to simply delete an app from the phone. As long as there is a user account system in place that requires data to be uploaded, all or most of the user data will automatically be stored on a cloud server controlled by the service provider. This includes location history, photos of the child, safezones (typically "home", "school"),

58 https://myxplora-uk.zendesk.com/hc/en-gb/articles/115000421894-User-manual-XPLORA-app
59 Mnemonic 2017, "Security Assessment of GPS Watches for Children"

name, and so on. If the device is no longer being used, and for example is resold, it is important that users are allowed to delete their accounts completely, and that doing so also removes all of that user data from the cloud server. Disappointingly, none of the four services allow account deletion. Since it seems impossible to delete an account, it is reasonable to believe that the data will in fact be kept indefinitely, even after the user has stopped using the service. If this is the case, this is an infringement of European data protection laws as service providers should delete personal data when storage is no longer necessary to provide the service to the user.[60]

Security in processing and storage

When a service provider collects and processes personal data, it has a responsibility to keep this data secure. In particular, users should be able to expect adequate security measures in devices meant for children, since children are particularly vulnerable, and the devices are meant to provide added safety. Data protection legislation differs between different areas of the world, so it is also important that the data controllers ensure that they process and store the personal data of European users in countries that have sufficient privacy protections (having passed a so-called adequacy decision).[61] The security practices and data flow of the devices and services are examined in detail in the technical report written by Mnemonic.[62] As most users do not have the possibility to examine the security in detail, it is important that the security of the services is brought up in the relevant user terms.

60 Directive 95/46/EC – article 1 cf. article 6 and article 12

61 http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

62 Mnemonic 2017, "Security Assessment of GPS Watches for Children"

Tinitell is the only service provider to mention security in their user terms, promising that:

> *"We take commercially reasonable security measures to protect your personal information (including, preventing the loss, misuse, unauthorized access, disclosure, alteration and destruction of your personal information)."*

Tinitell privacy policy

However, Tinitell does not mention where any collected personal data may be stored. The terms for Viksfjord/SeTracker, which is a Chinese-developed device and service, state that location data will be transmitted to Anquanshouhu Technologies' servers, without specifying where the servers are located:

> *"Using the SeTracker watch (...) will regularly report location information to Anquanshouhu Technologies Ltd servers."*

Viksfjord/SeTracker privacy policy

The Xplora terms are vague about where exactly personal data is kept, only stating that they use Amazon Web Service for cloud storage:

> *"All personal information received by you is subject to processing by Amazon Web Service on our behalf and we sometimes handle transfers of personal information to countries outside where you reside."*

Xplora privacy policy

Other problematic issues

The right to privacy is enshrined in the United Nations convention on human rights, and children are afforded special protections under the Convention on the Rights of the Child.[63] By continuously monitoring the location and even conversations of children, this right may be put under pressure. In Norway, the use of smartwatches for children has been criticized by both the Ombudsman for Children,[64] the Data Protection Authority, and Save the Children,[65] citing the potentially negative effects that surveillance may have on children's development, and the false sense of security that such devices might provide.

63 Convention on the Rights of the Child, Article 16 http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx

64 https://barneombudsbloggen.wordpress.com/2016/04/28/gps-sporing-av-barn-er-ikke-greit/

65 https://www.nrk.no/livsstil/_-falsk-trygghet-a-spore-barna-med-gps-pa-skoleveien-1.13103688

The “monitoring” function of the Viksfjord device/SeTracker app is in itself problematic. Even if one agrees that it should be permissible to listen in on children without their knowledge, the function enables you to monitor anyone in the vicinity of the child. This means that the Viksfjord can potentially be used to spy on the conversations of unwitting people.

Conclusion

After testing the four smartwatches and apps, and reading relevant user terms, it seems clear that this is a chaotic and somewhat immature market. In addition to unclear and/or illegal user terms, and lack of compliance with data protection legislation, the actual security features of three of the four devices fail to function as advertised. As products that are marketed toward parents in order to ease their worries, it is cause for concern that functions such as geofencing and SOS buttons are unreliable or simply do not work. The vast variety of products being imported and sold under different names also makes it exceedingly difficult to understand who is responsible for any problems with the devices or apps. The large number of disconcerting and potentially critical technical flaws discovered by Mnemonic further exacerbates these issues. Any consumer looking for ways to keep their children safe and secure might want to think twice before purchasing a smartwatch as long as the faults outlined in these reports have not been fixed.

Company establishments in Europe/ Norway selling the various smartwatches

Gator 2

Gator AS
https://www.gatornorge.no/

Håkon Magnussons Gate 8
7041 Trondheim
Norway

Organization number: 817 870 902
https://w2.brreg.no/enhet/sok/detalj.jsp?orgnr=817870902

Tinitell

Tinitell AB
http://tinitell.com/

Gävlegatan 12B
113 30 Stockholm
Sweden

Organization number: 556941-1514
(search word "Tinitell AB" on https://foretagsfakta.bolagsverket.se/fpl-dft-ext-web/home.seam?cid=233623)

Viksfjord

Etterforsker1 AS (trademark: GPS For Barn – https://gpsforbarn.no/)

Gokstadveien 18
3216 Sandefjord
Norway

Organization number: 913 193 458
https://w2.brreg.no/enhet/sok/detalj.jsp?orgnr=913193458

Xplora

Pepcall AS
https://xplora.no

Bryggegata 9
0250 Oslo
Norway

Organization number: 814 499 022
https://w2.brreg.no/enhet/sok/detalj.jsp?orgnr=814499022

User terms

Gator

No terms

Tinitell

Privacy policy:
http://tinitell.com/privacy-policy/

Viksfjord/SeTracker

Privacy policy:
http://en.3g-elec.com/index.php?c=content&a=list&catid=23

Xplora

Privacy policy:
https://s3-eu-west-1.amazonaws.com/support.pepcall/privacy/nb/privacypolicy.html

CLASSIFICATION: PUBLIC

Security Assessment Report
GPS Watches for Children
The Norwegian Consumer Council

18.10.2017

Harrison Sand <harrison@mnemonic.no> (Lead investigator)
Merete Løland Elle <merete@mnemonic.no>
Erlend Leiknes <erlend@mnemonic.no>
Tor E. Bjørstad <tor@mnemonic.no>

mnemonic
- securing your business

Summary

In cooperation with the Norwegian Consumer Council's "*Digilab" project*, mnemonic has performed a technical security assessment of four smart GPS watches for children. At the time of writing, the smart watches featured in this report are all readily available in both physical Norwegian retail stores, and are also marketed abroad.

The purpose of the assessment has been to provide an independent review of the security of these Internet connected devices, and evaluate whether they provide a *reasonable* level of privacy and security for their users. Ensuring an adequate level of security for the information processed and transmitted by these devices is particularly important, since they are intended to be used by children (and their parents).

A secondary goal has been to shed light on the risks associated with the rapid spread of Internet connected devices, often referred to as the "Internet of Things". There is a rapidly expanding presence of these devices in our daily lives, and as a result an unprecedented level of data generation, collection, transmission, and processing. In many cases, the data generated classifies as *personal data* or *personally identifiable information* (PII) and may be subject to privacy laws in many jurisdictions.

When such user data is not handled with due care and consideration, there may be serious implications to the privacy and potentially also to the safety and well-being of the users.

Our testing has discovered significant flaws in three of the four devices tested, which may lead to information about GPS watch users' location and activities ending up in the wrong hands. This technical report outlines our main findings and illustrates the associated risks through misuse scenarios.

About the assessor

mnemonic helps businesses manage their security risks, protect their data and defend against cyber threats. Our expert team of security consultants, product specialists, threat researchers, incident responders and ethical hackers, combined with our Argus security platform ensures we stay ahead of advanced cyberattacks and protect our customers from evolving threats.

Acknowledged by Gartner as a notable vendor in delivering Managed Security Services, threat intelligence and advanced targeted attack detection, we are among the largest IT security service providers in Europe, the preferred security partner of the region's top companies and a trusted source of threat intelligence to Europol and other law enforcement agencies globally.

With intelligence-driven managed security services, more than 150 security experts, and partnerships with leading security vendors, mnemonic enables businesses to stay secure and compliant while reducing costs.

Table of Contents

1 Introduction

mnemonic has carried out technical testing of four smart GPS watches marketed towards children and their parents. The testing has been carried out as part of the Norwegian Consumer Council's "*Digilab*" project.

The key feature of the smart watches is that they allow parents to track their children's movements. This is combined with mobile phone functionality, which can be used to maintain contact with the child. Each watch contains a GPS receiver and an embedded SIM card, and position data is transmitted continually to the vendors' back-end servers. The wearer's location can then be tracked via a companion app, which typically shows the position on a map.

At the time of writing, the watches featured in this report are all readily available for purchase in Norway, both in physical stores and on-line. Some of the models are available internationally, sometimes marketed under different brand names.

The different watches support additional features, depending on the model. Examples include two-way voice communication, camera, geo-fencing (a function that sends alerts if the devices leaves a predefined boundary), alarms, and more.

Three of the four watches that were tested were found to contain significant security flaws. The flaws are not technically difficult to exploit, and in two cases, allow a third party to surreptitiously take control over the watch. This technical report describes our main findings.

1.1 What has mnemonic evaluated

mnemonic has evaluated the technical security of the watches and their mobile apps in our testing lab. Our goal has been to explore what kind of information and access what somebody with hostile intent might be able to get from a watch that they do not own, based on logical or technical vulnerabilities in the design and implementation of the watches, as well as their supporting infrastructure (back-end services and mobile apps).

When discussing information security in consumer products, it can be difficult to quantify the expected level of security. Indeed, there are few technical standards in this area, and the law does not mandate specific technical safeguards. Our general expectation is that end users, who in most cases will not have the technical expertise to evaluate the security of their devices on their own, should not be at significant risk when using device default settings and/or following the instruction manual.

We have based our tests on four more specific expectations that we think are *reasonable* expectations in terms of data security:

1. For someone who does not own a watch, it should be unfeasible to gain access to any user data.
2. For somebody who does own a watch, it should only be feasible to access their own user data.
3. Data transmitted over the public Internet should be protected by encryption to prevent user information from being visible while the data is in transit.
4. Supporting infrastructure should not have any *obvious* security holes, i.e. flaws that can be identified *passively* by observing the systems, without performing any (potentially illegal) active "hacking" activities.

These are not the *only* security properties that may be relevant in a consumer perspective, but they provide a good starting point for further analysis and discussion. The testing has thus been an attempt to investigate whether these assumptions hold in practice.

Testing has mainly been carried out on the Android version of the mobile apps. We do not anticipate major differences in terms of security between the Android and iOS versions of the apps.

1.2 Ethical considerations

When investigating the security and safety of widely used products, there is an ever-present ethical dilemma that must be taken into account, namely that of responsible disclosure.

- By publicly disclosing detailed vulnerability information, there is a risk that "bad guys" (or simply "honest but curious" parties) will actively use this information – potentially causing harm to users – before the users have a chance to become informed and protect themselves.
- By *not* publicly disclosing vulnerabilities, there is a risk that vendors will not prioritize fixing the problem. There is also a continual risk that the same vulnerabilities will be independently re-discovered by dishonest actors. Finally, end users are unable to protect themselves by taking informed decisions regarding the security of their personal data.

In the Internet of Things setting, this problem is magnified by the fact that devices are marketed and sold worldwide, and that end users often have limited possibilities to react. For a typical "smart" device, it may not even be feasible for end users to carry out security updates on the devices even if a patch were to be made available.

To balance these concerns, and in order to reduce the short-term risk of exploitation and harm, key technical details have been redacted from the initial public release of this report.

Redacted sections of the report are marked as follows:

Redacted Content

Due to significant risk of other researchers independently replicating our results, we strongly urge the device manufacturers to take immediate steps to protect their customers and their customers' data.

We also advise all users of the affected devices to take precautionary actions immediately. Parents should strive to understand the security issues that are present in the smart watches, and the potential consequences for their children's privacy and security, to make an informed choice about whether and how a smart watch should be used. mnemonic recommends following the advice of consumer protection agencies about how to react.

As vendor updates and security fixes for the watches become available, they should be installed immediately. Instructions on how to proceed should be provided by the device vendors.

The following disclosure timeline has been followed by mnemonic:

- August 21st, 2017: Start of initial test phase. Ongoing communication between mnemonic and the Norwegian Consumer Council (NCC).

- September 1st, 2017: Findings disclosed to the Norwegian Data Protection Authority (DPA), Datatilsynet.
- September 12th, 2017: Formal notifications sent by the Norwegian DPA to the respective Norwegian product distributors and/or manufacturers. European and international points of contact were also notified (where applicable), as well as the national DPAs in France and England.
- September 13th, 2017: Communications established between the DPA and all Norwegian product distributors.
- October 5th, 2017: Received information from product distributors (via DPA) that mnemonic's findings will be addressed before planned release of report.

Detailed technical information about the findings has been provided by mnemonic to each of the responsible parties, to ease analysis and remediation. However, mnemonic has not verified, nor endorsed, these fixes.

1.3 Structure of the report

Chapter 1 (the current chapter) provides the overall context of the report.

In Chapters 2 and 3, we present the devices that we have tested, as well as our overall testing approach. Building on the general information, Chapter 4 presents some of the main attack scenarios that we have been able to demonstrate in the lab. Chapter 5 goes into additional detail on some of our more general findings. Finally, we provide some meta-data about the report in Chapter 6.

An appendix is included, which describes additional technical observations.

2 The GPS Watches

The GPS watches all have the same basic interaction pattern. Each watch contains a SIM card, which is used to transmit location data (and possibly other information) over 2G / Edge to a back-end service residing in the cloud.

A companion smartphone app is used to monitor the watch's movements by retrieving data from the cloud service API. The app must be paired with the watch as part of initial setup. Figure 1 shows the overall data flow between watch, back-end, and app.

Figure 1. High level data flow between watch, back-end, and app.

We have tested the Xplora, Viksfjord, Gator 2 and Tinitell TT1 watches. These are all models that are marketed and sold in Norwegian stores. Most of our tests have been carried out using the Android version of the apps, though the apps are also available for iOS.

2.1 Xplora

Manufacturer	Infomark / Pepcall AS
Country of origin	South Korea
Retail price	1 995 NOK ($260 USD)
Purchase location	Spaceworld
App Name	Xplora T1
Android package	kr.co.infomark.kidzon.pcbeta
App version	1.1.8
Other names	JooN2

2.2 Viksfjord (SeTracker family)

Manufacturer	Wonlex / gpsforbarn.no (Etterforsker1 AS)
Country of origin	China
Retail price	1 999 NOK ($260 USD)
Purchase location	Enklere Liv
App Name	SeTracker
Android package	org.zywx.wbpalmstar.widgetone.uexaaagg10003
App version	4.2.6
Other names	Various, available from Aliexpress for $30 USD

Note: *Viksfjord* is the Norwegian name for a specific GPS watch which belongs to a larger family of watches that all use the same back-end infrastructure and the *SeTracker* mobile app for control. However, there are a variety of models, and they are marketed internationally under a wide variety of names.

Some of the functionality varies between different watches in the SeTracker family. For instance, the *Stavern* watch, which is also sold in Norway has a built-in camera, whereas the Viksfjord does not.

We have conducted most of our tests on the Viksfjord watch, but have also had a brief look at some of the other models. As far as we have been able to determine, all of our findings with respect to the Viksfjord watch appear to apply to the entire SeTracker family of watches.

2.3 Gator 2

Manufacturer	Techsixtyfour / Gator Group Co. / GatorNorge
Country of origin	China
Retail price	1 199 NOK ($150 USD)
Purchase location	XXL
App Name	Gator
Android package	com.gatorgroup.carefwatch
App version	2.5.20
Other names	Caref (North America)

Note: The Gator 3 and Caref watches were also briefly tested to verify if the same findings were present. Additional comments are given in in *4.6 Note on the Gator Family* .

2.4 Tinitell TT1

Manufacturer	Tinitell AB
Country of origin	Sweden
Retail price	1 490 NOK ($190 USD)
Purchase location	Kjell & Company
App Name	Tinitell
Android package	com.tinitell.tguardian
App version	1.14.0
Other names	none

3 Testing Methodology

We have mainly utilized four techniques to assess the devices: data-flow analysis, source code analysis, analysis of data at rest, and hardware analysis.

Data-flow analysis

Under ordinary circumstances, an app will communicate directly with the web services it requires. This is not an ideal scenario if we are interested in analyzing these types of communications. In order to obtain a better vantage point, we utilize a web proxy that's situated between the mobile device and access out to the internet.

When the app makes a request for data in the lab setting, it is first passed to our web proxy and then forwarded along to its intended destination. This gives us the ability to see exactly what the application is sending and receiving, in addition to complete control over the flow of data.

We have configured our proxy and mobile device to support both the inspection of encrypted traffic, and use of additional protection mechanisms such as certificate pinning.

Source code analysis

Understanding how an application works is key to assessing security. One method to better understand an application is to review its code and see how it was built. Application code can reveal security flaws, hidden functionality, and provide insight into the developers' thought process. We have in some cases been able to reverse-engineer and analyse the underlying code to aid our understanding.

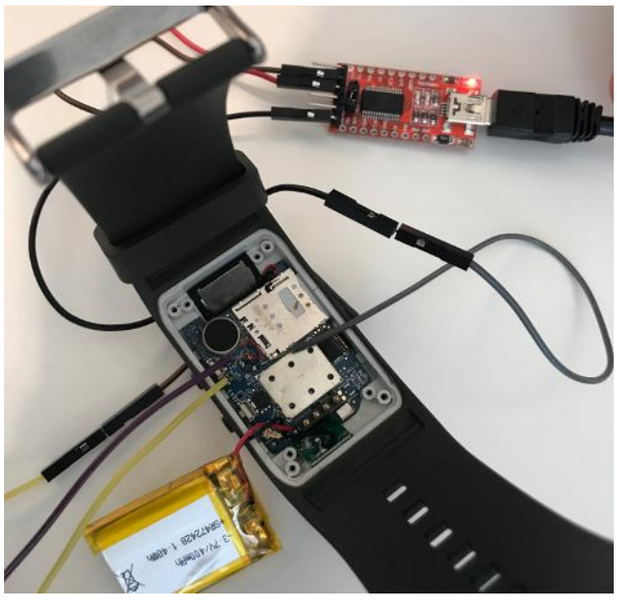


Figure 2. Assessing debug interfaces on the Tinitell.

Analysis of Data at Rest

Applications can store significant amounts of information locally on a mobile device. Just like an ordinary computer, storing data in an insecure manner on mobile devices can be a liability if that device is lost, stolen, or compromised. It is therefore important to ensure that apps properly secure sensitive data at rest.

Hardware Analysis

Hardware can be a valuable source of information. Debug interfaces and device firmware can both provide new attack vectors and information about the device and how it operates.

4 Practical attack scenarios

Our security testing has resulted in multiple serious and practical attacks on the Gator 2, Viksfjord (SeTracker family), and Xplora watches. The attacks are based on combinations of security vulnerabilities and more general design flaws. This section describes the main attack scenarios that we have found.

4.1 Covert Account Takeover (Gator 2)

A combination of critical design flaws in the Gator 2 leaves accounts vulnerable to compromise. This attack does not require interaction from the user, and can be performed without raising suspicion to the account owner or child that unauthorized activity has occurred.

This attack can be performed by anybody possessing a basic to moderate understanding of web communications. Due to the ease of execution, it is a plausible assumption that this attack could have already been discovered by another party and be in active use. It would also be possible to automate and sell to non-technical users.

4.1.1 Obtaining an IMEI

A prerequisite for this attack is to have knowledge of the Gator watch's IMEI: a number assigned to mobile devices that serves as a unique identifier and used by Gator during the account registration process.

We have identified four ways to obtain an IMEI for use in attacks against both targeted and random devices. Three of these do not require physical access to the device.

1. Physical access to the device.

   The IMEI is printed on the back of the device and on the interior of the device packaging.

Figure 3. Rear side of Gator 2 watch, displaying the device's IMEI.

Additional techniques have been redacted for the initial release of the report.

Redacted Content

4.1.2 Account Registration

As part of the account registration process, Gator relies on the user submitting the IMEI of the device they would like to associate with their account. If the device has been previously registered, Gator's server will return some information about the device and the account that it has already been associated with, as shown in Figure 4.

The next paragraphs have been redacted for the initial release of the report.

Redacted Content

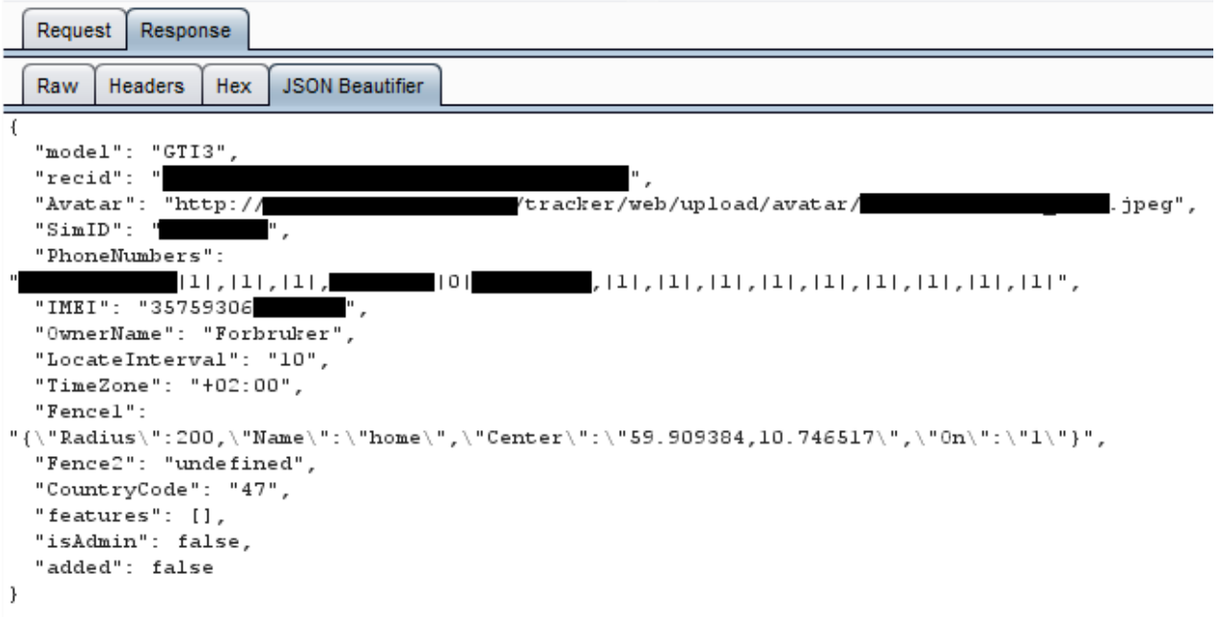


Figure 4. Response from Gator's server, including sensitive account information.

Even before adding the watch to our account, we have acquired the following information:

- The account's "avatar", which could presumably be a photo of the child
- The phone number of the watch
- Whitelisted phone numbers in the watch's contact list, including names
- Name of the user (child)
- Geofence locations set in the app (home, school, etc.)

4.1.3 Account Verification

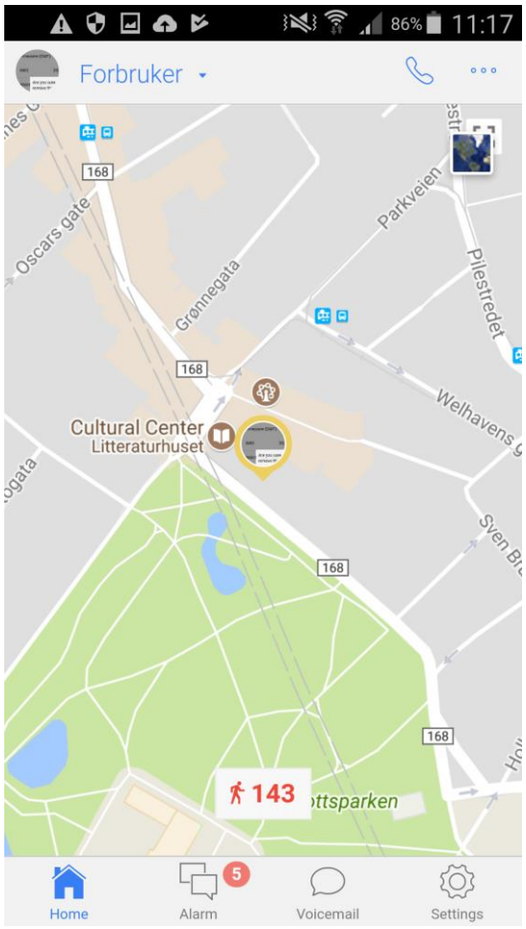
Another serious flaw in the Gator 2 lies in the account verification process. When a user attempts to add a watch that has already been associated with another account, they are prompted to enter a verification code that's located in the settings page of original account owner's app.

Despite the verification code process, we are successfully able to pair the watch to our account without being in physical possession of the watch, and without the watch owner knowing we have connected the watch.

The next paragraphs have been redacted for the initial release of the report.

Redacted Content

As shown in Figure 5, logging out and back into the app will reveal that we have successfully paired the watch with our account.



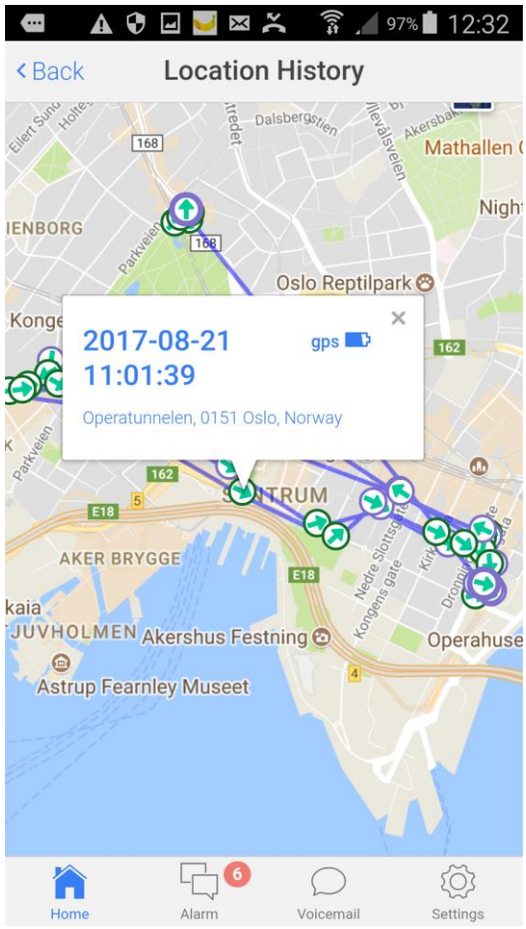


Figure 5. After pairing the watch with our account, we have access to live and historic location data.

After pairing, we now have full access to the device, which includes:

- Current location of the watch
- Location history, including timestamps
- The ability to send and receive voice messages to the watch
- Editing or removing geofences
- Editing or removing phone numbers in the contact list

4.1.4 Protecting against the attack

A serious concern with our attack, and the set of vulnerabilities and design flaws that we have discovered in the Gator 2, is that we cannot see a good way for users to protect themselves at present.

Even if users stop using the watch completely, there is no functionality available to delete accounts or account history. Discontinuing use of the Gator 2 watch will only prevent further data generation and exposure, but will not prevent an attacker from accessing historical data already recorded. Even by using the "Delete this watch" function provided, it only un-pairs the watch from the account, but does not delete account history. Because of this, an attacker can re-pair the watch with their own account and access all data ever associated with the watch.

While testing the attack, we did not receive any indication of authorized activity on either the "legitimate" test account, or on the watch. There were no emails or other alerts received when we paired the watch with a second account. At the time of our tests, we did not find a way for users to detect that somebody has carried out a similar attack as ours, and is able to eavesdrop on their device and data.

Thus, we conclude that until the Gator back-end server is either patched or taken offline, anybody who has purchased and activated the Gator 2 watch will be vulnerable to our attack.

Based on our understanding of the product, it appears very difficult for Gator to successfully patch and secure their service to a level that reasonably protects customers, without a major redesign of the Gator 2 product, back-end service, and mobile app. Although it cannot be ruled out, it seems unlikely that such changes would be compatible with existing devices that have already been sold.

4.2 Covert Account Takeover (Viksfjord)

Similar to the attack on the Gator 2 described in the previous section, we have identified an attack against the Viksfjord/SeTracker family of watches. Based on our tests, knowledge of the device IMEI or phone number leads to a complete compromise of the user account and gives an attacker full access to the device.

Additionally, anybody with physical access to the device is able to pair the watch to their account, as the registration code is printed on the back of the watch.

Figure 6. Rear side of Viksfjord watch, displaying the device's registration code.

The Viksfjord verification functionality differs from what we saw when testing the Gator 2. Pairing a Viksfjord watch to the app required a registration code, and not an IMEI like the Gator 2. There are no additional steps required to pair a watch with an account, the registration code is all that is required.

The next paragraphs have been redacted for the initial release of the report.

Redacted Content

mnemonic has developed a method to reliably generate registration codes for the SeTracker watches.

All four methods we identified for obtaining an IMEI with the Gator 2 also apply here.

4.2.1 Protecting against the attack

Similar to the account takeover attack with the Gator 2, we see no way for consumers to protect themselves. Discontinued use will only prevent active tracking of the watch and further collection of data.

Data already stored by that app will be available for an attacker to access, as we have not found any functionality for users to delete their historical data.

Given the large and complex SeTracker watch ecosystem, it seems particularly challenging to update the devices to offer reasonable privacy safeguards, while maintaining compatibility with existing devices.

The next paragraphs have been redacted for the initial release of the report.

Redacted Content

4.3 Location Spoofing (Gator 2, Viksfjord)

Both the Gator 2 and the Viksfjord (SeTracker family) watches are vulnerable to a man-in-the-middle attack, which allows an attacker to manipulate location data sent from the watch back to manufacturer's back-end servers. This effectively makes the watch appear to be in a different location than it actually is, as shown in Figure 7.

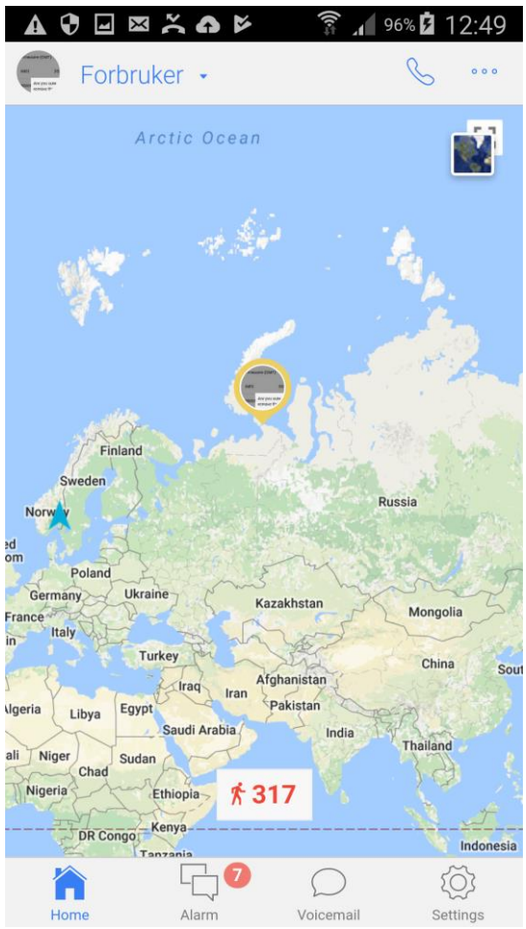


Figure 7. Altering data sent back to Gator's server makes the watch appear to be in Siberia instead of Oslo.

The attacker is also able to monitor the *real* location data, turning the watch into an effective tracking device.

The next paragraphs have been redacted for the initial release of the report.

Redacted Content

This attack is similar to the previous in that it can be performed without alerting the target, and could feasibly be automated and used by non-technical users.

4.4 Misusing Voice Call Functionality (Viksfjord)

The Viksfjord allows anybody to instruct the watch to call back a specified number. No interaction on the watch is required to initiate the call. This effectively turns the device into a remotely controllable listening device, or alternately provides means for an attacker to communicate directly with the child.

The next paragraphs have been redacted for the initial release of the report.

Redacted Content

When a covert phone call is initiated, a "Call forwarding on" notification is briefly displayed on the device, as shown in Figure 8. There are no indications that such a call has taken place visible in the parents' app.

Figure 8. A notification is displayed on the Viksfjord before initiating our call.

This attack can theoretically be prevented by the app user, by using an undocumented feature of the device to reset a default password. This functionality is not described in the documentation we received with the device. We would not expect the average consumer to be aware of the fact that this feature exists, nor be able to change the setting on their own.

A variant of the attack could be to instruct the watch to dial special fee-based numbers in order to steal money from account holders. There is also a similar function which can be used by an attacker to instruct the watch to send SMS messages, further increasing the attack potential.

4.5 Sensitive Data Disclosure (Xplora)

While conducting our assessment of the Xplora watch, we inadvertently came across sensitive personal data belonging to other users Xplora users, including location data, names, and phone numbers.

Due to the nature of this vulnerability, it is not possible to go into additional detail until we are certain that the flaw has been fixed.

The remainder of this section has been redacted for the initial release of the report.

Redacted Content

4.6 Note on the Gator Family of Watches

Similarly to the Viksfjord / SeTracker family of watches, the Gator watch exists in multiple variants.

We briefly assessed the new Gator 3 watch, which has recently arrived in Norway, as well as the Caref watch which is sold in North America, to determine if our findings for the Gator 2 are applicable to these.

As this was a limited-scope assessment aimed towards the verification of known findings, we did not search for new or changed vulnerabilities. As such, the results of this section do not constitute an in-depth security assessment of the Gator 3 and Caref.

The Gator 3 watch is an updated version of the Gator 2 watch and shares many similarities with the previous version, despite its updated hardware and use of a different app. We found the Gator 3 to be vulnerable to the same findings as the Gator 2, with the exception of the account takeover attack described in 4.1, due to changes in the way the app communicates with its backend infrastructure.

The Caref watch is a version of the Gator watch sold in North America. This watch has slightly different hardware, and a separate app and backend infrastructure. Due to the changes in the app and backend infrastructure, the only finding we were able to reproduce for the Caref watch is the location spoofing attack described in 4.3.

5 General Observations

5.1 Build quality and usability

A general concern with the Gator 2 and Viksfjord watches is that the overall quality appears to be quite poor. While our test was not focused on usability and durability, we would have expected more solid devices, particularly given the high price tag, and noting that the intended users are children who may be likely to give the watch a rough treatment.

The apps had stability issues during testing, with frequent crashes and sometimes requiring manual restarts. Basic functionality, such as geofencing and SOS seemed quite unreliable, with alerts only being sent intermittently.

The build quality and overall design of the Gator 2 was somewhat noteworthy, as it requires extensive disassembly to install the SIM card, exposing sensitive internal electronics. Additionally, the USB charger of the Gator 2 uses a proprietary standard which broke during our testing, requiring the purchase of a new watch.

Figure 9. To install a SIM card in the Gator 2, you first have to disassemble the watch.

The perceived functional and build quality of the Xplora and Tinitell watches was noticeably better, despite being the same price or less expensive than the other watches.

5.2 Data Privacy and Security

As described in Chapter 4, we found vulnerabilities in three of the watches leading to leakage of customer data. Within our limited test window, we did not discover explicit security vulnerabilities in the Tinitell device.

However, none of the devices handle data privacy and security particularly well. The inherent nature of the GPS watches means that they collect, transmit, and store large amounts of information about its user's movements – indeed, that is their main purpose. In our opinion, it is obvious that this information should be treated securely and with proper respect for users' privacy. However, this is not the case in practice.

We observed that all the devices we tested communicated with more than one back-end service, and many sent large amounts of data back to third parties. For the Gator 2 and the Tinitell, some of the back-end services were not encrypted, which means that it would be possible for somebody listening to the network communications to eavesdrop on this data.

Several devices also collect information you wouldn't necessarily expect them to, including lists of nearby WiFi hotspots, and usage information like what buttons you press within the app.

Another concern is the third parties that this data is sent to. Several of the devices send data back to obscure servers around the world, with little indication as to how that information is stored, secured or used on the back-end.

We have included a table of communications we identified while testing as an appendix to this report. See *Appendix B – Overview of Application Communications*.

5.3 Device and Application Security

5.3.1 Application Permissions

Both iOS and Android utilize app permissions to limit the access apps have to a device. Following the principle of least privilege, app permissions are designed to ensure apps can only access functions they require. Users will typically encounter this functionality when installing an app, or when attempting to perform a specific function like using the camera.

When creating an app, developers have to specify which permissions they want given to their app. Following their intended purpose, best practice is only request permissions that the application will actually use. For example, an application shouldn't request permission to send SMS messages if there's no legitimate requirement to send SMS messages.

Overly liberal permissions increases an applications attack surface, and can leave users vulnerable to a variety of security issues. However, the Tinitell was the only device we tested that limited the permissions it requested to those it actually required.

See *Appendix A – Application Device Permissions* for a detailed list of permissions that each app requested in our tests.

5.3.2 [Redacted]

This section has been redacted in full for the initial release of the report.

Redacted Content

5.3.3 Unencrypted Local Storage

We noted that the Tinitell and Viksfjord stored location data and cookies locally on the phone, unencrypted.

Cookies could be used by an attacker to gain access to an account without knowledge of the account's password.

5.4 Backend Applications and Infrastructure

Though an assessment of the infrastructure supporting these devices was out of our scope, we passively noted several serious areas of concern that potentially expose sensitive customer information.

5.4.1 [Redacted]

This section has been redacted in full for the initial release of the report.

Redacted Content

5.4.2 [Redacted]

This section has been redacted in full for the initial release of the report.

Redacted Content

6 About the document

6.1 Test execution

Performed by:	mnemonic AS
Lead investigator:	Harrison Sand
Consultants:	Merete Løland Elle, Erlend Leiknes
QA and editing:	Tor E. Bjørstad
Client:	The Norwegian Consumer Council
Started:	2017-08-21
Ended:	2017-10-10

6.2 Document version control

The current version of this document is 1.0.

The table below contains a brief description and version number of the document. All major changes are documented in this table.

Rev	Date	Consultant	Comments
1.0	2017-10-10	mnemonic team	Approved for release
0.99	2017-10-05	Tor E. Bjørstad	Final QA
0.9	2017-10-03	Harrison Sand	Minor revision
0.8	2017-09-21	Tor E. Bjørstad	Internal QA
0.7	2017-09-19	Harrison Sand Merete Løland Elle	Major revision
0.5	2017-08-30	Harrison Sand	Draft shared in meeting with DPA
0.1	2017-08-28	Harrison Sand	First internal draft

Appendix A – Application Device Permissions

Below is a table of device permissions that each of the application requested access for. These are the same permissions as a user accepts when installing an app from the Google Play Store, though presented in a more detailed format.

Information about individual permissions and what they allow can be found on Android's developer portal: https://developer.android.com/reference/android/Manifest.permission.html

Android Permission	Viksfjord	Xplora	Gator 2	Tinitell
ACCESS_COARSE_LOCATION	x	x	x	
ACCESS_FINE_LOCATION	x	x	x	x
ACCESS_NETWORK_STATE	x	x		x
ACCESS_WIFI_STATE	x	x		
BLUETOOTH	x			x
BLUETOOTH_ADMIN	x			x
CALL_PHONE	x	x	x	x
CAMERA	x		x	
CHANGE_CONFIGURATION	x			
CHANGE_WIFI_STATE	x		x	
FLASHLIGHT	x		x	
GET_ACCOUNTS	x	x	x	
GET_TASKS		x		
INTERNET	x	x	x	x
MANAGE_ACCOUNTS	x			
MODIFY_AUDIO_SETTINGS		x		
MOUNT_UNMOUNT_FILESYSTEMS			x	
READ_CONTACTS	x	x	x	x
READ_EXTERNAL_STORAGE	x	x		x
READ_PHONE_STATE	x	x	x	
READ_PROFILE		x		
RECEIVE_BOOT_COMPLETED		x	x	
RECEIVE_WAP_PUSH		x		
RECORD_AUDIO	x	x	x	x
RECORD_VIDEO			x	
REORDER_TASKS		x		
SEND_SMS			x	
SYSTEM_ALERT_WINDOW	x			
VIBRATE	x	x	x	
WAKE_LOCK	x	x	x	x
WRITE_CONTACTS			x	
WRITE_EXTERNAL_STORAGE	x	x	x	
Total	**22**	**20**	**19**	**10**

Appendix B – Overview of Application Communications

The below table lists the different back-end services that the mobile apps communicate with. For each mobile app, the following properties of each identified service are listed: Internet address (hostname and IP address), the registered owner of the domain name, the physical location of the servers, the hosting provider, whether communications are encrypted, and what kind of data is sent.

Each of the apps has its own back-end service for application data and location data, and uses Google for map data. But in addition to this, several other services have been identified. In some cases, we have also found that data is sent unencrypted over the network, which means that the transmissions are not private.

Hostnames and IP-addresses have been redacted for the initial release of the report.

Hostname	Domain Owner	IP(s)	Physical Location	Hosting Provider	Encrypted	Data
Xplora						
[Redacted]	Infomark Co.,Ltd.	[Redacted]	Ireland	Amazon	Yes	Application data, location data
[Redacted]	Google	Anycast DNS[1]	Worldwide	Google	Yes	Map data
[Redacted]	Google	Anycast DNS	Worldwide	Amazon	Yes	Error reporting
Viksfjord						
[Redacted]	wenchangrong, HiChina Web Solutions Limited, 250881995@qq.com	[Redacted]	Frankfurt, Germany	Amazon	Yes	Application data, location data
[Redacted]	Google	Anycast DNS	Worldwide	Google	Yes	Map data
Gator 2						
[Redacted]	Chen jiaren, chenjiaren711@126.com	[Redacted]	Toronto, Canada	iWeb Dedicated CL	No	Application data, location data
[Redacted]	Google	Anycast DNS	Worldwide	Google	No	Map data

[1] Anycast DNS is a technology that returns a different (usually nearby) IP address and service location, based on the user's geographic location.

Hostname	Domain Owner	IP(s)	Physical Location	Hosting Provider	Encrypted	Data
[Redacted]	Baidu	[Redacted]	Hong Kong	Baidu	No	Location data
[Redacted]	SKYHOOKWIRELESS	[Redacted]	Singapore	Amazon	Yes	Nearby WiFi access points
Tinitell						
[Redacted]	Mats Horn, Tinitell	[Redacted]	Ashburn, Virginia	Amazon	Yes (w/ certificate pinning)	Nearby WiFi access points, location data, application data
[Redacted]	Private (assuming Mixpanel)	Anycast DNS	Worldwide	Mixpanel, Inc.	Yes	Device metadata and application usage information
[Redacted]	Liao Ben, kellychen@generalmobi.com (Taiwan)	[Redacted]	Singapore	Amazon	No	Device and app metadata, IMEI, firmware updates
[Redacted]	Google	Anycast DNS	Worldwide	Amazon	Yes	Error reporting
[Redacted]	Google	Anycast DNS	Worldwide	Google	Yes	Map data

FOR MORE INFORMATION

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

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