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.

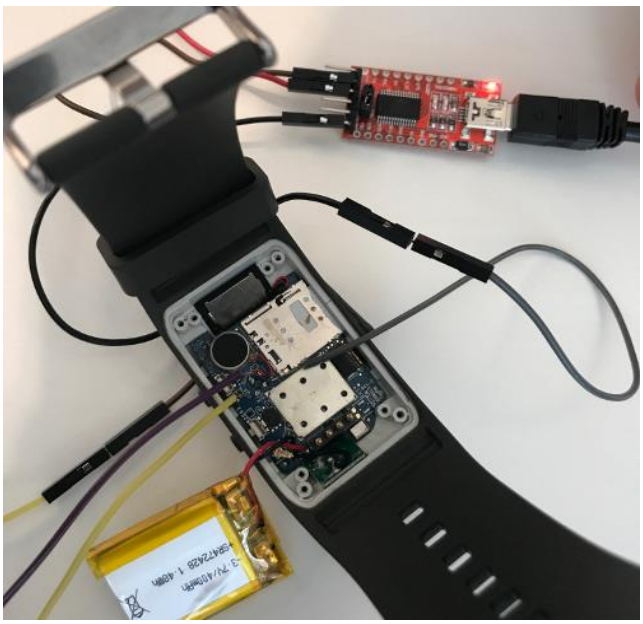

Figure 2. Assessing debug interfaces on the Tinitell.

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

Request | Response

Raw | Headers | Hex | JSON Beautifier


```
{
  "model": "GTI3",
  "recid": "[redacted]",
  "Avatar": "http://[redacted]/tracker/web/upload/avatar/[redacted].jpeg",
  "SimID": "[redacted]",
  "PhoneNumbers":
"[redacted]|1|,|1|,|1|,[redacted]|0|[redacted],|1|,|1|,|1|,|1|,|1|,|1|,|1|,|1|,|1|",
  "IMEI": "35759306[redacted]",
  "OwnerName": "Forbruker",
  "LocateInterval": "10",
  "TimeZone": "+02:00",
  "Fence1":
"{\"Radius\":200,\"Name\":\"home\",\"Center\":\"59.909384,10.746517\",\"On\":\"1\"}",
  "Fence2": "undefined",
  "CountryCode": "47",
  "features": [],
  "isAdmin": false,
  "added": false
}
```


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.

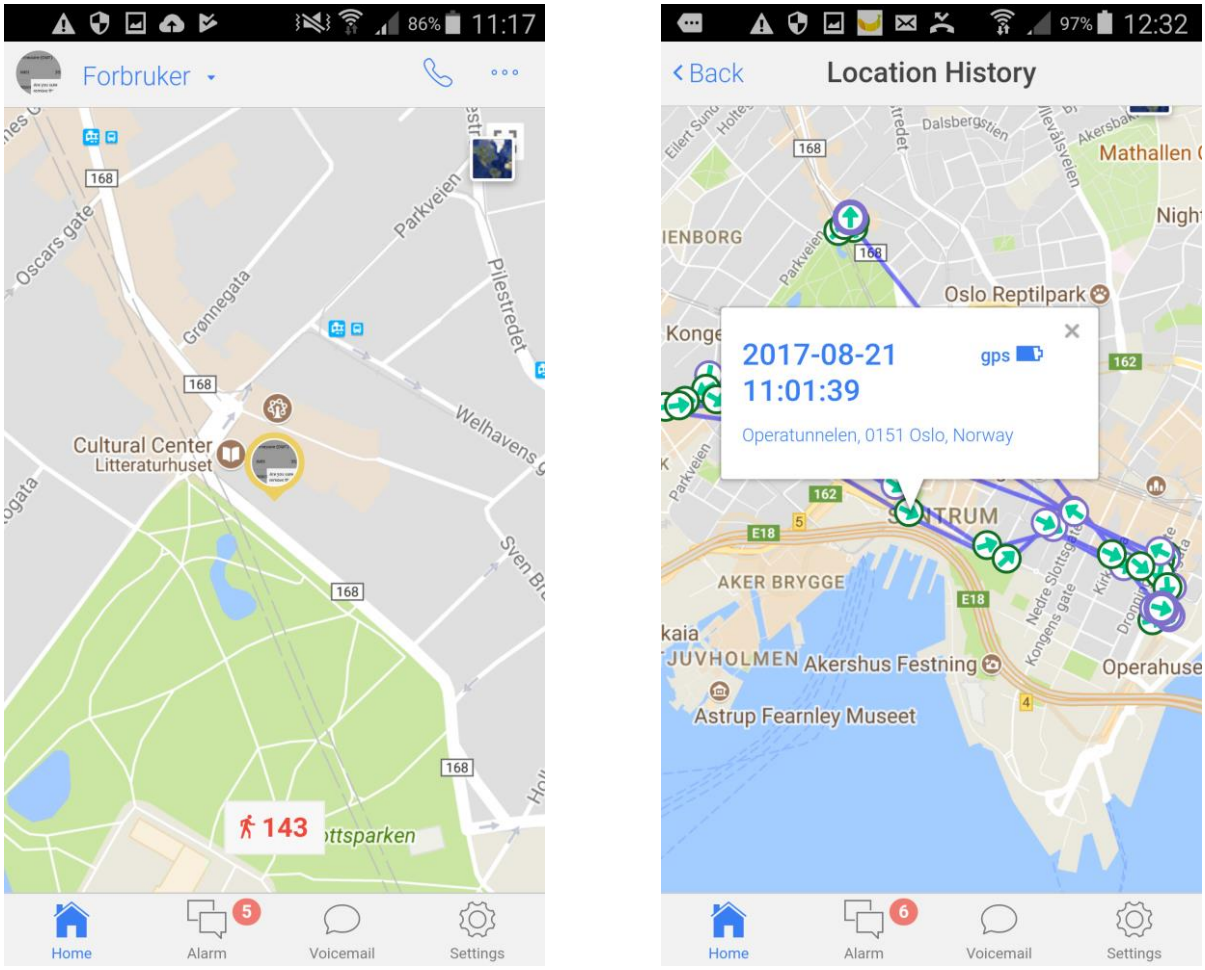

Figure 5. After pairing the watch with our account, we have access to live and historic location data.

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.

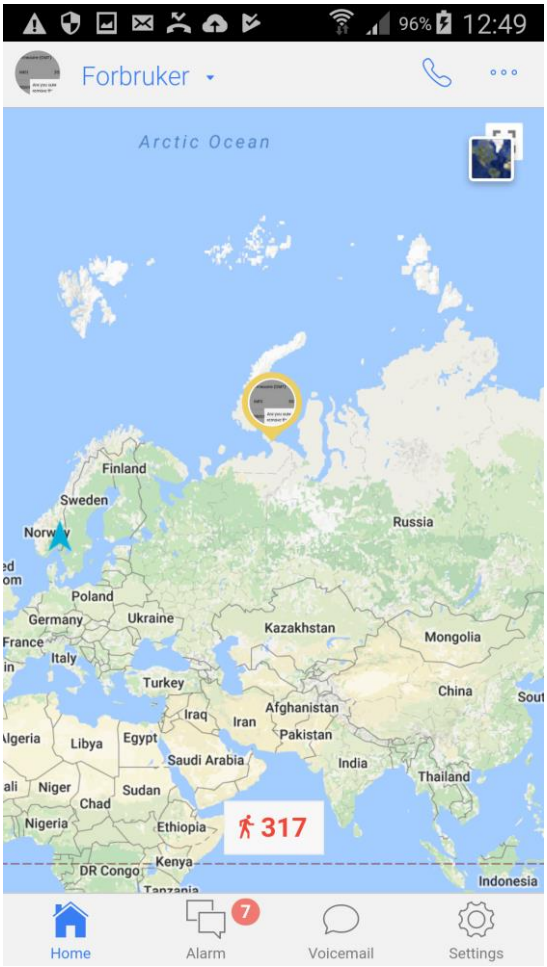

Figure 7. Altering data sent back to Gator's server makes the watch appear to be in Siberia instead of Oslo.

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