



26 November 2017

PRELIMINARY REPORT

AllMyTribe Spacetalk Watch

REVIEW OF SECURITY AND PRIVACY

On Wednesday 22 November 2017 I was contacted by Mark Fortunatow, CEO of MGM Wireless Holding Pty Ltd, and commissioned to conduct a detailed review of Security and Privacy aspects of the Spacetalk children's GPS smart watch phone product and its associated ecosystem.

SCOPE OF WORKS

The final report will consider:

- Technical security mechanisms implemented in the AllMyTribe ecosystem to protect user privacy. This review will consider technical documentation provided by the company, interviews with technical staff of the company, and some penetration testing (technical experimentation).
- Compliance with relevant policy and regulations in the Australian market, including such matters as informed consent, legal requirements for retaining customer records and measures required to secure private information.
- Other matters related to user safety and device security.
- Recommendations related to the security and privacy framework to support the evolution of the product and ecosystem.

The draft report is due on 15 December 2017, while the final report, including recommendations related to the product evolution, is due on 23 February 2018.

It is the intention that reports will be made public, although some technical details may be redacted for commercial-in-confidence reasons.

In line with best ethical practice, if security defects are identified, the company will be informed immediately so that remediation can be put in place before public disclosure.

MY CREDENTIALS

I have over 19 years of experience teaching, developing and consulting in the areas of telecommunications and multimedia engineering, and have been a tenured member of academic staff at the University of Adelaide since 2002. I am currently Senior Lecturer in the School of Electrical and Electronic Engineering.

I hold a PhD in Information Technology from George Mason University (1998), a Bachelor of Engineering in Computer Systems (1993) from the University of Adelaide, a Bachelor of Science in Theoretical and Experimental Physics (1992) from the University of Adelaide, and a Graduate Certificate in Management from the University of Adelaide (2002).

Since 2005, my primary areas of research have been in the forensic analysis of digital images and video, with specific focus on artifacts and limitations introduced by digital capture and

compression processes; and more recently on related areas of electronic device security and forensics, cyber defence and cyber crime with some experience in internet security and cryptanalysis. I have acted as an expert or provided technical support in a number of criminal and civil cases in South Australia, and I currently provide investigative consulting services to a number of law enforcement agencies.

In 2008 and 2009 I chaired the “e-Forensics: Forensic Applications and Techniques in Telecommunications, Information and Multimedia” international conference in Adelaide.

Since 2013 I have been an invited academic observer at the United Nations Office of Drugs and Crime Intergovernmental Experts Panel on Cybercrime in Vienna, Austria.

In 2017 I was appointed as an academic member of the INTERPOL Digital Forensics Expert Group, specialising in wearable devices such as smart watches and fitness devices.

I am currently actively engaged in research collaboration in cyber-security and digital government with the Tallinn University of Technology in Tallinn, Estonia.

PREVIOUS ENGAGEMENT WITH MGM WIRELESS

In 2003, the Convergent Communications Research Group at the University of Adelaide, of which I was then Research Director, was commissioned by Ezyimage Ltd to prepare an independent expert valuation report of MGM Wireless Holdings Pty Ltd. I also supervised an Honours student project in that year, sponsored by MGM Wireless, to explore the then-emerging Multimedia Messaging Service.

PRELIMINARY OBSERVATIONS

On 18 October 2017, the Norwegian Consumer Council (Forbruker Rådet) released a detailed report which identified serious privacy and security flaws in four GPS-enabled watches for children available in the Norwegian market. That report – with some redaction – is publicly available at <https://www.mnemonic.no/news/2017/watchout/>.

The findings of that report against the reviewed devices are not disputed and will be used to benchmark the Spacetalk Watch and some competitor products in the Australian market. It is believed that the competitor products in Australia may be the same OEM products available in the Norwegian market, although this has yet to be confirmed.

As a first stage in the evaluation of the Spacetalk Watch, the key findings list of that report are considered to identify whether there are comparable defects – including serious technical or compliance defects, in that product. That summary is annexed to this statement.

Of particular relevance is that MGM Wireless Ltd’s Privacy Policy is written to comply fully with the Australian Privacy Principles¹ in line with their current market. Privacy is more tightly regulated in Europe and there are some differences in regulated record-keeping requirements. Hence, consideration has been given to the required compliance under Australian regulation as well as hypothetical compliance under European principles *if the Spacetalk Watch were to be released in European markets*.

As a broad preliminary summary, the issues raised in the Norwegian Consumer Council Report have been appropriately addressed in the implementation of the Spacetalk Watch in the context of the Australian market. A small amount of additional ecosystem development would be required to meet the regulatory requirements in Europe.

In keeping with best practice, MGM is adopting a process of continuous monitoring, improvement and public disclosure of the Spacetalk Watch in terms of its functionality,

¹ Privacy Fact Sheet 17: Australian Privacy Principles, available at <https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles>, accessed 26/11/17

security and privacy. This approach ensures rapid discovery, assessment and rectification in the event that a security defect is identified, and maintains public trust by timely disclosure. It is emphasised that a preliminary review of the implementation of the Spacetalk ecosystem suggests that none of the serious technical flaws identified in the watches reviewed in Norway are evident.

A handwritten signature in black ink, appearing to read 'M. Sorell', written in a cursive style.

Dr Matthew Sorell
Senior Lecturer

ANNEX: Preliminary Evaluation of AllMyTribe Spacetalk Watch against the Norwegian Consumer Council findings

Summary of Terms (Page 5 of the NCC report)		
Consent is sought at registration	AU: COMPLIANT	The Privacy Policy ² is explicitly referenced in the registration process in compliance with Australian Privacy Principles. It is recommended that more explicit informed consent be implemented, especially in a European market context
I will be notified if the terms are changed	YES	MGM has undertaken to email registered users of the AllMyTribe app, and registered account holders, of changes to policies including End User Licence Agreements, Privacy Policy, etc. To date these terms have not changed.
My personal data will not be used for marketing purposes	YES	Specified in the Privacy Policy APP-8 (page 6)
I can delete data in the app	AU: COMPLIANT DEVELOPMENT IN PROGRESS	I understand these features are in development. They are not required under Australian privacy principles and may be restricted in scope by the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015. These features would require implementation for the European market.
Location data is automatically deleted after a set period of time		
I can delete my user account	YES	However, account deletion requires manual intervention by the company
Promises to implement reasonable security standards	YES	Specified in the Privacy Policy APP-11 (page 8)
It is made clear where personal data is transmitted and stored	YES	Specified in the Privacy Policy APP-8 (page 6) and in other documentation that all personal data remains within, and is stored and processed in, Australia. Alternative data housing arrangements may be required for other markets.

As a further observation, anonymity is protected by the option for end users to use pseudonymous identifiers to access the AllMyTribe app and child identifiers. However, under Australian law, mobile phone accounts, which are used to access the Spacetalk Watch and the AllMyTribe app on a parent’s smartphone, are required to be linked to a verifiable identity.

² MGM Wireless Privacy Policy, at https://mgmwireless.com/downloads/MGM_Wireless_Customer_Privacy_Policy.pdf, accessed 26/11/17

Features of the device (Page 8)		
Make/receive calls	YES	Calls can only be made and received with numbers on the Contact List, which is maintained through the AllMyTribe app by the parent. Calls with no caller ID are blocked.
Contact list	YES	
GPS tracking in app	YES	Transmission of location information to the parent-managed app is a key feature of the product. Secure transmission protocols are used to protect against interception of location data.
Geofencing	YES	
SOS button	YES	This is a simple process for the child to make contact in case of emergency
Receive SMS	YES	SMS can only be received from sources on the contact list. Of note is that notifications from the 3G mobile carrier regarding prepaid credit will not be received, but these messages will be interpreted by the AllMyTribe server and the end user notified through the app.
Voicemail	NO	However it is technically possible to set up voicemail through the mobile service provider.
Monitoring	NO	Surveillance through the device is generally illegal without the informed consent of the parties to the conversation.
Alert if device is removed from arm	NO	These features are not supported, in line with the <i>Privacy rights of children and young people at international law</i> ³ . In short, children have the right to choose not to be tracked and to protect their own privacy.
Prevent child from turning off device	NO	

Technical Assessment

The Spacetalk watch has not yet been tested against the technical security assessment conducted by **mnemonic** for the Norwegian Consumer Council and annexed to that agency's report, dated 18 October 2017. Preliminary discussions with engineering staff at MGM Wireless, and review of technical documentation provided to date, suggest that the technical exploitation weaknesses identified in **mnemonic**'s report have been considered and addressed in the design and implementation of the Spacetalk watch.

³ Decision Making by and for Individuals Under the Age of 18, at <https://www.alrc.gov.au/publications/68.%20Decision%20Making%20by%20and%20for%20Individuals%20Under%20the%20Age%20of%2018/privacy-rights-children->, accessed 26/11/17