ASX Announcement

MGM Wireless Limited (ASX:MWR)

**19th March 2018**

# International Cyber Security Audit Finds SPACETALK Provides Superior Security and Safety

- Independent, international cyber security audit validates SPACETALK and AllMyTribe ecosystem's claims as most secure family smartwatch phone reviewed
- INTERPOL-accredited global expert's report commends MGM's engineering team for world-leading best practice security, encryption and authentication
- SPACETALK does not exhibit any of the technical weaknesses identified and investigated in a European review of similar devices.

**19th March, 2018** - **MGM Wireless Limited (ASX:MWR)** On 18th October 2017, the Norwegian Consumer Council published a report identifying serious privacy and security flaws in four GPS-enabled watches for children[1]. Following this report, MGM Wireless ('MGM', 'the Company') commissioned an in-depth review of security and privacy aspects of its SPACETALK children's GPS smart watch phone and All My Tribe (AMT) ecosystem, by Dr Matthew Sorell, of the School of Electrical and Electronic Engineering at University of Adelaide.

A recognised cyber security expert, Dr Sorell was appointed last year as an academic member of the INTERPOL Digital Forensics Expert Group, specialising in wearable devices such as smart watches and fitness devices. He conducted a review of SPACETALK's technical security mechanisms and compliance with policy and regulations in the Australian market, encompassing informed consent, legal requirements for retaining customer records, and measures required to secure private information.

Dr Sorell has now completed his systematic investigation and delivered his comprehensive 33-page report which concludes:

- All My Tribe ecosystem uses best practice security for authenticated and encrypted communications between subsystems, and best practice identity authentication.
- MGM's commitment to well-engineered security solutions and ongoing security development is to be commended.
- Overall, **technical security of the SPACETALK Watch and the All My Tribe ecosystem is implemented well and is appropriate for purpose**.

[1] https://www.mnemonic.no/news/2017/watchout/

- Recommendations are to further enhance the AMT ecosystem in readiness for European privacy requirements, in particular EU GDPR.

"In conducting this work, I have had full and frank access to and disclosure from MGM's engineers," Dr Sorell said. "No aspect of the All My Tribe system was off limits. I commend MGM's best practice approach to this review.

**"This report goes further than my preliminary report in November 2017 – I have since found that the SPACETALK Watch and ecosystem do not exhibit any of the technical weaknesses identified and investigated in the Norwegian review of similar devices."**

Dr Sorell said that a child's smartwatch design should ensure that the rights to privacy and self-determination of children are balanced with the responsibilities of their parents. This includes emergency response and ensuring that well-informed consent to track the child is given.

"Overall, the technical security and privacy measures implemented in the All My Tribe ecosystem exceed what I would consider to be the contemporary levels of security appropriate for All My Tribe as it exists today, and provides some breathing space for future development," Dr Sorell said.

Dr Sorell points out that no IT system is entirely immune to a sufficiently determined attacker. A properly configured security framework is multi-layered, incorporating best practice defences; monitoring and notifications; proactive means for staying informed about emerging security threats; effective mechanisms for users to report bugs and issues; and a timely, open and public discussion about security and privacy product developments.

"MGM's commitment to well-engineered security solutions and ongoing security development are to be commended," he said.

MGM Wireless CEO Mark Fortunatow said that SPACETALK had been designed with the highest levels of data security and privacy from the ground up. He congratulated Dr Sorell on a very detailed and comprehensive report.

Dr Sorell has recommended development improvements to avoid any opportunistic threats now and in future. The recommendations include ongoing responses to the changing security threat landscape, as well as product safety enhancements to empower Australian children and families.

An extracted public summary of Dr Sorell's final report is attached to this announcement.

**Co-Founder, Chairman & CEO Commentary**

**MGM Wireless Co-Founder, Chairman & CEO Mark Fortunatow:**

"Throughout MGM's 17 year history of working with schools, we have gained a very deep understanding of the importance of data security and privacy requirements that any technology associated with children must have.

"Further, we believe that as a supplier of technology for children and families, we have moral and social responsibilities that transcend commercial issues alone.

"Suppliers of children's products have a responsibility to ensure that 'under the hood' , their products are safe and properly built for children.

"This type of responsibility with a brand new technology such as a children's smartwatch phone, may not be written into legal obligations, but it is baked into every one of MGM products.

"When you're dealing with children and students, their safety, security and well-being are of upmost importance. Technology providers have a duty of care to ensure their products are secure, safe and protect the welfare of students and families at all times.

"We are delighted that this independent report has validated our strategy to maintain the most stringent and best-practice security practices."

**ABOUT DR MATTHEW SORELL**

**Dr Matthew Sorell** had over 19 years of experience teaching, developing and consulting in the areas of telecommunications and multimedia engineering, and has been a member of academic staff at the University of Adelaide since 2002. He is currently Senior Lecturer in the School of Electrical and Electronic Engineering.

He holds a PhD in Information Technology, Bachelor of Engineering in Computer Systems, Bachelor of Science in Theoretical and Experimental Physics, and Graduate Certificate in Management.

Since 2005, his primary areas of research have been in the forensic analysis of digital images and video, with specific focus on artefacts 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.

He has acted as an expert in a number of criminal and civil cases in South Australia, and currently provides investigative consulting services to a number of law enforcement agencies.

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

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

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

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

In 2018 he was shortlisted for the International Digital Investigation & Intelligence Awards, sponsored in the United Kingdom by the National Police Chiefs Council, for "Contribution(s) to Developing Emerging Sources of Digital Investigation", specifically in relation to investigative work involving wearable devices.

Dr Matthew Sorell, School of Electrical and Electronic Engineering, University of Adelaide

Email: matthew.sorell@adelaide.edu.au Phone (mobile): +61 410 432 762

**ABOUT MGM**

MGM Wireless Limited is a technology company designing, developing and commercialising Internet of Things (IoT) devices for children, and software for school communication and student absence management. The Company's AllMyTribe division has developed a wearable device called SPACETALK, which allows two-way 3G communication, GPS tracking and alerts parents whenever children leave designated safe spaces, such as school or the home.

MGM Wireless built its track record with school communication solutions after creating the world's first SMS based Automated Student Absence Notification Solution. It is recognised as a global leader and pioneer in socially responsible and technology-enabled school communications.

MGM Wireless products include student absence notifications 'messageyou', absence analytics software 'Watchlists', school news and messaging app 'School Star', a content management and messaging platform for mobile school communication called Outreach+, and student attendance management solution 'RollMarker'.

Used by over 1100 schools and 1.6 million parents, the Company's multichannel school communication solutions empower schools to effectively communicate to parents and caregivers through SMS, mobile in-app and other means to improve student attendance and safety, help schools reduce operating costs and increase parent engagement.

To learn more please visit: www.mgmwireless.com

**For more information please contact:**

**MGM Wireless Limited**

Mark Fortunatow, CEO

mfortunatow@mgmwireless.com

M: +61 421 328 984




**-Ends-**

THE UNIVERSITY of ADELAIDE

# Security Report
# AllMyTribe Spacetalk Watch

Report prepared by

11 March 2018

Dr Matthew Sorell
School of Electrical and Electronic Engineering
University of Adelaide

Email: matthew.sorell@adelaide.edu.au

Phone (mobile): +61 410 432 762

# Public Summary

## REVIEW OF SECURITY AND PRIVACY

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/.

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 All My Tribe (AMT) ecosystem.

## SCOPE OF WORKS

The final report considers:

- Technical security mechanisms implemented in the AMT 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.

In conducting this work, I have had full and frank access and disclosure with MGM's engineers. No aspect of the All My Tribe system was off limits. I commend MGM's best practice approach to this review.

In addition, a number of validation experiments were conducted, through which a small number of relatively minor security weaknesses were identified. These do not constitute a significant security threat but development improvements are recommended in the body of the report.

As the body of the report contains frank recommendations which are commercial-in-confidence, only this summary will be made public.

The recommendations include requirements for ongoing responses to the changing security threat landscape, as well as product development recommendations which further enhance the watch as an empowering safety device for Australian children and families.

A preliminary report, released on 26 November 2017, identified that **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.**

I commend the Norwegian authors for their thorough review and their frank disclosure of the shortcomings of devices available in the Norwegian market.

This report goes further, identifying that the Spacetalk Watch in the AMT ecosystem does not exhibit any of the technical weaknesses identified and investigated in the Norwegian report in similar devices.

Overall, **technical security of the Spacetalk Watch and the All My Tribe ecosystem is implemented well and is appropriate for purpose.** Some precautionary confidential recommendations have however been made to further improve technical security.

Further recommendations have been made to ensure that the rights to privacy and self-determination of children are balanced with the responsibilities of their parents. This includes providing highly accessible resources which clearly explain how the watch works, ensuring that consent to track the child is given with the best available understanding.

There are further recommendations in the body of the report concerning scalable features to respond to emergency situations.

## DISCUSSION

The technical security review has identified that the AMT ecosystem uses best practice security for authenticated and encrypted communications between subsystems, and best practice identity authentication using the Open ID Connect.

No Information Technology system is entirely immune to a sufficiently determined attacker. A properly configured security framework is multi-layered, incorporating best practice defences; monitoring and notifications; proactive means for staying informed about emerging security threats; effective mechanisms for users to report bugs and issues; and a timely, open and public discussion about security and privacy product developments. MGM's commitment to well-engineered security solutions and ongoing security development is to be commended.

Effective lock-outs have been implemented to minimise the risk of a watch device or account being intercepted, diverted, or taken over by an attacker. Engineering and test modes and reporting in the watch have been effectively disabled so that these are not available through the watch interface.

A minor security weakness was identified which can cause a parent not to be notified when the watch is switched off, for which a simple fix has been implemented.

Further, specific recommendations were made to ensure the watch supports access to emergency services (000 or the international 112 emergency number). Changes have been implemented to significantly improve emergency call support.

It has been determined that minimal personal information is stored on the watch as necessary for the effective operation of the watch. I understand minimal personal information is stored in the AMT server, noting however that this includes historical location information which requires escalated security.

Recommendations have been made concerning data retention and a user's right to have records deleted on request. These recommendations are intended to respect the privacy of the individual while meeting legal data retention requirements.

The Australian Privacy Principles[1], which form the base of MGM's Privacy Policy[2], apply. Particular attention should be paid to the APP Guidelines[3] which states that:

---

[1] Australian Privacy Principles, at https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles, accessed 9/2/18.
[2] MGM Wireless Privacy Policy, https://mgmwireless.com/downloads/MGM_Wireless_Customer_Privacy_Policy.pdf, accessed 9/2/18.
[3] Australian Privacy Principle Guidelines, https://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP-guidelines-combined-set-v1.pdf, accessed 9/2/18

> *As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.*

It is recognised that the features in the Spacetalk Watch have been specifically chosen to minimise interference to the child's right to privacy while also providing an effective means of communication and reassurance for the child and the parent.

For example, it is noted that some competitor watches feature a covert listening mode. Using such a feature is not only an invasion of the child's privacy, it is also *illegal* under the relevant Surveillance Devices Act (or equivalent, on a federal and/or state-by-state basis) in most contexts. AMT therefore, correctly, has both not developed such a feature and has taken steps to minimise the risk of the device being used in a covert listening manner.

Further, it is noted that a camera has not been implemented in the Spacetalk watch. It is recommended that should a camera be included in a future generation Spacetalk watch, strong measures be taken to prevent covert, undisclosed or unauthorised transmission of images or video from the camera.

One key recommendation on consent and disclosure is to provide highly accessible disclosures which clearly explain to children how the watch can track their location, so that both parents and children can provide effective and conscious informed consent.

It is also recommended that potential users have access to clear explanation that the Spacetalk Watch should not be used in restricted areas (such as military bases), nor for prominent public families who face a significantly higher security risk than the generally public.

Further, it should be recognised that in a custody and access dispute context, the watch may provide a means for tracking an estranged former partner by proxy through the child's trackable movements. Such tracking may be illegal under relevant surveillance devices legislation and potential purchasers should be explicitly advised not to use the device in this way.

Finally, a number of recommendations have been made to improve a child's independent access to emergency services without requiring the intervention of the parent, and to ensure that emergency services can respond and investigate effectively.

It should also be noted that some competing devices in the Australian market have been reviewed and tested for comparison. The results of these tests will be disclosed to relevant parties before being made public.