

Potential Liability of WhatsApp Admins: A Critical Appraisal of the Legal Position in Malaysia

Nazli Ismail Nawang

Faculty of Law and International Relations, Universiti Sultan Zainal Abidin, Kampus Gong Badak, 21300 Kuala Nerus, Terengganu

Noor 'Ashikin Hamid

Faculty of Law and International Relations, Universiti Sultan Zainal Abidin, Kampus Gong Badak, 21300 Kuala Nerus, Terengganu

Nur Amani Pauzai

Faculty of Law and International Relations, Universiti Sultan Zainal Abidin, Kampus Gong Badak, 21300 Kuala Nerus, Terengganu

To Link this Article: <http://dx.doi.org/10.6007/IJARBSS/v8-i12/5242>

DOI:10.6007/IJARBSS/v8-i12/5242

Published Date: 07 January 2018

Abstract

The recently published Digital News Report 2017 by Reuters Institute for the Study of Journalism has discovered the rise of instant messaging applications such as WhatsApp, Viber, WeChat, Line and many others for sharing and distributing of news in the cyber world. Out of these services, WhatsApp was found to have been the preferred platform in Malaysia with over half of the surveyed respondents in the country (51 percent) used the application for news. The scenario has undoubtedly raised a serious cause for concern regarding the spread of fake news among WhatsApp users. In relation to this, the Deputy Minister of Communications and Multimedia, Datuk Jailani Johari, has on 27 April 2017 reprimanded WhatsApp admins that as gatekeepers they may be exposed to legal actions including imprisonment, should they fail to control and prevent the spread of false information that could jeopardise national security among members of WhatsApp groups that they administer. Nonetheless, uncertainty arises as to the legality of this move as it seems to hold WhatsApp admins accountable not only for their own posts, but also for any false information that are disseminated by other members in their groups. As such, this article attempts to analyse relevant statutory provisions related to the proposed move and the potential liability of WhatsApp admins for illegal postings made by other group members.

Introduction

WhatsApp is a messaging application that offers free text services and free mobile calls over the Internet. It was founded by Jan Koum and Brian Acton in 2009 primarily as an alternative

to the traditional paid short message service (SMS). Unlike social networks such as Facebook or Twitter which are easily accessible and open to a broad audience, WhatsApp enables the sharing of content including simple chats, photos and videos in a more private and secured channel. Apart from that, WhatsApp accords group chat feature that allows its users to share content with up to 256 group members at once. Perhaps due to its closed and secured architecture, Business Insider reported that WhatsApp and many other messaging services like Viber, WeChat, Line etc. have surpassed the popularity and usage of social networks in the cyber world (Business Insider, 2016). Out of these messaging services, WhatsApp was found to have been the most preferred platform in Malaysia with over half of the survey respondents in the country (51 percent) used the application for sharing news (Centre for Independent Journalism, 2012).

Nonetheless, the widespread acceptance and use of WhatsApp has been misused by unscrupulous individuals to spread false news and other prohibited materials in WhatsApp groups. Since the occurrence of these incidents are on the rise, the Deputy Minister of Communications and Multimedia, Datuk Jailani Johari, has on 27 April 2017 reminded WhatsApp admins that they may be exposed to legal actions including imprisonment, for their failure to control and prevent the spread of false information that could jeopardise national security in WhatsApp groups that they administer (Berita Harian Online, 2017). The proposal was however met with strong opposition from various quarters in the society, in particular WhatsApp admins and also its users, as it seems to hold WhatsApp admins accountable for false information or other illegal content that are disseminated by other members in their groups. Thus, it is pertinent to critically examine relevant statutory provisions in Malaysia that may be applicable to communications in WhatsApp.

Communications and Multimedia Act 1998 (CMA)

In general, all communications in the cyber world are not left unregulated as they come under the purview of the Communications and Multimedia Act 1998 (CMA). The CMA was specifically enacted to cater for the convergence of three different industries, namely the broadcasting, telecommunications and IT industries that were previously regulated by separate statutes. With the passage of the CMA, these industries are now being grouped as a 'new communications and multimedia industry' and subjected to a single regulatory framework under the CMA. In overseeing the operation of the converging industry, the government has established a new regulatory body, the Malaysian Communications and Multimedia Commission (MCMC), pursuant to the Malaysian Communications and Multimedia Commission Act 1998 (MCMCA). The MCMC is a single regulator entrusted to regulate and supervise the communications and multimedia industry as well as other services which come within the ambit of the Postal Services Act 1991 and the Digital Signature Act 1997. As such, the Commission is regarded as a super regulator for all types of media but the print industry, which is still subjected to the provisions of the Printing Presses and Publications Act 1984 (PPA).

With regard to the regulation of online content, any content published in the electronic environment is bound by the provisions of the CMA. Section 6 defines the word 'content' as 'any sound, text, still picture, moving picture or other audio-visual representation, tactile representation or any combination of the preceding which is capable of being created, manipulated, stored, retrieved or communicated electronically'. This definition is all-inclusive

so as to embrace any materials published electronically including via WhatsApp. As such, all WhatsApp users should be aware of the prohibitions contained in the CMA. Section 211(1) provides that it is a criminal offence to provide online content which is 'indecent, obscene, false, menacing or offensive content with intent to annoy, abuse, threaten or harass any person'. Such offence carries a maximum fine of RM50,000 or one year imprisonment or both. Apart from prohibition on provision of offensive content, improper use of network facilities, network services or applications service to transmit illegal content is also not permitted. Section 233(1) states that the use of any facilities or services to transmit content which is 'obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another' would amount to a criminal offence which carries a fine of not exceeding RM50,000 or one year imprisonment or both. It is thus submitted that any WhatsApp users who are found to have violated the aforesaid provisions may be charged either under section 211 or section 233 of the CMA. Nonetheless, so far only section 233 has been reported in law journals whilst no single case on section 211 has of to date been reported.

Among the earliest case involving prosecution under section 233 of the CMA is the case of PP v. Chan Hon Keong ([2012] 5 LNS 184). The accused was charged with posting obscene remarks and offensive comments against Sultan Azlan Shah on the official website of Sultan Perak with the intention of upsetting the Sultan and his people. The court has, after taking into consideration various aspects of the case, sentenced the accused to a maximum of 12 month imprisonment and a fine of RM50,000. In the subsequent case of PP v. Muslim Ahmad ([2013] 5 CLJ 822), the respondent faced three charges under section 233(1) of the CMA for making offensive comments on the official website of the Perak State Government. The respondent was initially released by the court of the first instance as the prosecution failed to prove the case beyond reasonable doubt. However, the case was reversed on appeal and the High Court has convicted and sentenced the respondent to a fine of RM 10,000 for each charge, in default to six months imprisonment for each count.

In PP v. Rutinin Suhaimin ([2013] 2 CLJ 427), the case involved an appeal by the prosecution against the discharge and acquittal of the respondent at the end of the prosecution's case. The respondent was charged under section 233 of the CMA for posting an offensive remark on the online visitor book of the homepage of the Perak Sultan. The court of the first instance decided that there was no prima facie case against the respondent as the prosecutor failed to prove the offensive remark was indeed posted by the respondent and that the Internet could have been accessed by anyone from the disputed computer. On appeal, the acquittal was quashed and the respondent was ordered to enter his defence. It was ruled by Ravintran Paramaguru JC that the trial judge had failed to consider the strength of circumstantial evidence by forensic expert indicating that the Internet account belonged to the respondent and that there was no evidence that any other person had used the computer at the time of the offence. The accused was then tried before another Sessions Court judge and he was later convicted for the offence and was sentenced to a fine of RM 15,000, in default eight months' imprisonment. Dissatisfied with the decision, the accused (now the appellant) then lodged his appeal in *Rutinin Suhaimin v PP* ([2015] 3 CLJ 838) in the High Court of Kota Kinabalu, Sabah. On appeal, the appellant insisted that he did not make the offensive remark though it originated from his Internet account as his computer and the Internet account were accessible by other persons. It was observed by Richard Malanjum CJ that the trial judge had

erroneously held the defence as a mere denial as she failed to consider the appellant's defence on the whole. Further, she appeared to have shifted the onus of proof on the appellant to prove his innocence and this approach was totally unacceptable as there was no such presumption under section 233 of the CMA. Apart from that, there was not even an iota of evidence adduced by the prosecution to show that it was in fact the appellant who actually made and initiated the transmission of the offensive remark. As a result, the appeal was allowed and the earlier conviction and sentence were set aside as the appellant was found to have successfully raised a reasonable doubt in his defence.

The aforementioned decisions have clearly indicated that any kinds of communications in the cyberspace including via WhatsApp shall also be subjected to the express provisions of the CMA. This point may be best illustrated with the occurrence of recent cases whereby WhatsApp users have been remanded or detained pursuant to the alleged violation of section 233. For instance, in April 2017, a 48-year-old man was arrested for insulting government leader in WhatsApp (The Star Online, 2017). In another incident, a 76-year-old man was remanded for sharing a crude photo insulting the Prime Minister in a WhatsApp group (The Star Online, 2017). Nonetheless, the central issue that need to be addressed is whether WhatsApp admins could be legally held responsible for any unlawful content including fake news that are shared by other members in groups they administer. In relation thereof, it is pertinent to examine the provision in details.

Section 233 of the CMA stipulates two key elements that need to be proved before any legal action may be taken against WhatsApp admins. The first prerequisite is the alleged prohibited content should be knowingly made by the alleged offenders, and secondly the communication of such content should be coupled with the perpetrators' intention to 'annoy, abuse, threaten or harass another person'. For that reason, it is argued that since any members in WhatsApp groups may technically share and communicate any types of information without WhatsApp admins' approval, it seems to be difficult to prove the existence of knowledge of such unlawful content on WhatsApp admins. This is particularly true in groups with huge numbers of active members as it is almost next to impossible for WhatsApp admins to supervise or know each and every posting disseminated in such groups. And if the first element is hypothetically fulfilled, the prosecutor then needs to prove the existence of 'intention to annoy, abuse, threaten or harass another person' on the part of WhatsApp admins. In relation to this, it is submitted that the proposed move to inflict liability on WhatsApp admins for illegal content shared by other members of WhatsApp groups seems to be highly improbable as the authorities may face with an uphill task in meeting the statutory requirements of section 233. Nonetheless, certain quarters in the society have expressed their reservations on the potential application of this section as section 114A of the Evidence Act 1950 has statutorily established the presumption of fact in publication.

Section 114A of the Evidence Act 1950

Section 114A was inserted as a new amendment to the Evidence Act 1950 vide the Evidence (Amendment) (No 2) Act 2012. The amendment was tabled on 18 April 2012 and was passed without substantial debate on 9 May 2012. It has now come into force starting from 31 July 2012. Entitled as 'Presumption of Fact in Publication', the new statutory provision is similar to other presumptions that require the establishment of certain basic facts before such presumptions may be invoked by the court. Nonetheless, the passing of the amendment has

led to a heated debate among members of the public. The Centre for Independent Journalism has strongly objected to the new amendment on the perception that the presumption could lead to arbitrary arrest and prosecution of innocent persons (Centre for Independent Journalism, (2017). Ultimately, it was argued to be against the basic principles of a fair legal system which presume a person is innocent until proven guilty by the prosecution. It was further alleged that section 114A will have a serious chilling effect on freedom of speech and expression on the ground that members of the public may simply resort to self-censorship in order to avoid any unwarranted consequences. On the contrary, the proponent of this new amendment asserted that the enforcement agencies are still required to conduct comprehensive investigation to trace and identify the real suspects before making charges (The Sun Daily, (2012). This is in parallel with the explanation by the Minister in the Prime Minister's Department, Dato' Seri Mohamed Nazri Aziz, during the Parliamentary debate which expressly stipulated that the prosecution must prove the existence of certain specific facts before the rebuttable presumption of fact under section 114A may be invoked (Aziz, M. N. (2012).

Section 114A (1) states that "A person whose name, photograph or pseudonym appears on any publication depicting himself as the owner, host, administrator, editor or sub-editor, or who in any manner facilitates to publish or republish the publication is presumed to have published or re-published the contents of the publication unless the contrary is proved." Plain reading of the provision appears to presume any person as the publisher if his name, photograph or pseudonym is portrayed as the owner, host, administrator, editor or sub-editor of such online content. In relation to this, Peters argued that subsection (1) of section 114A may implicate online intermediaries or any other persons who administer, operate or provide online forums or discussion groups. It was further argued that they may possibly be held accountable for the content even if they have no knowledge about it once it is proved that they facilitate the publication of any disputed content (Peters, M. (2012). Apart from that, Radhakrishna alleged that the presumption may affect victims of hacking and identity theft and they would have to bear the evidential burden of proving their innocence (Radhakrishna, G. (2013).

Section 114A has been applied in the case of YB Dato' Hj Husam Hj Musa v Mohd Faisal Rohban Ahmad ([2015] 1 CLJ 787). The appellant sued the respondent for publishing articles defamatory of him on a blog 'ruangbicarafaisal.blogspot.com'. The trial judge found the articles were defamatory of the appellant, but still ruled in favour of the respondent on the ground that the appellant had failed to establish the respondent as the writer or owner of the blog without considering the coming into force of section 114A of the Evidence Act 1950. On appeal, it was ruled that the trial judge had failed to contemplate the application of the new amendment in the electronic environment as it will assist the appellant to force the respondent to exonerate himself from liability. Since the appellant had successfully linked the respondent to the defamatory posts via the latter's photographs and his letter to other bloggers, the first presumption under section 114A was accordingly invoked. Consequently, the appeal was allowed as the respondent had failed to rebut the presumption of fact and his defence of mere denial was not accepted by the court.

Section 114A has again been referred to in Ahmad Abd Jalil lwn PP ([2015] 5 CLJ 480). The appellant was convicted for posting offensive comments in Facebook using a pseudonym

account. The appellant then appealed against his conviction on a number of grounds including that the disputed computer from which the offensive remarks were published on the pseudonym Facebook account, though was under his control, could have been accessed by anyone in his office and thus the presumption of publication invoked by the prosecution under section 114A should have failed. Nevertheless, the appeal was dismissed as the High Court found that based on relevant circumstantial evidence and forensic experts presented by the prosecution, the appellant had failed to rebut the presumption on a balance of probabilities.

Based on the aforesaid judgments, it is apparent that the court would only permit the application of presumption of publication by the prosecutor (in criminal cases) or plaintiff (in civil suits) after the existence of relevant facts has been clearly established. Only then, the burden will be shifted to the offender to prove his innocence on a balance of probabilities. With regard to the implication of this provision to WhatsApp, any admins may be deemed to have issued a prohibited communication within the group they control although they are unaware of the status of the communications which are made by other members. However, the application of section 114A to impose liability on WhatsApp admins is arguably inappropriate and would be contrary to the main objective of this provision which intends to address the issue of anonymity in the virtual world.

Conclusion

To sum up, it is important to highlight that the role played by WhatsApp admins is not the same as editors of printed publications like newspapers or periodicals as they are responsible and duty bound to check and verify the truth and validity of any facts and information before being published. The technical design of WhatsApp application however permits members in WhatsApp groups to share any communication without first procuring permission or approval from WhatsApp admins. As a result, it would be difficult for WhatsApp admins to know or be aware of the authenticity of all the communications within the group that they control. Therefore, it is submitted that it would be inappropriate to impose liability for the dissemination of false news within the WhatsApp group by other members on WhatsApp admins. Further, such culprits who are responsible to spread out any prohibited communications in WhatsApp groups can be possibly identified and tracked either by admins or other members as well as the enforcement agencies. However, this position will definitely change if such unlawful content is indeed disseminated by WhatsApp admins themselves as they may be presumed to have the required knowledge and intention as per stated in section 233 of the CMA.

Corresponding Author

Nazli Ismail Nawang, Faculty of Law and International Relations, Universiti Sultan Zainal Abidin, Kampus Gong Badak, 21300 Kuala Nerus, Terengganu, Malaysia.

E-mail: nazlismail@gmail.com

References

Ahmad Abd Jalil Iwn PP [2015] 5 CLJ 480

Aziz, M. N. (2012). Malaysian Hansard House of Representatives – Parliamentary Debates. Retrieved May 13, 2017 <http://www.parlimen.gov.my/files/hindex/pdf/DR-18042012.pdf>

- Business Insider. (2016, September 20). Messaging apps are now bigger than social networks. Retrieved August 11, 2017, from <http://www.businessinsider.com/the-messaging-app-report-2015-11/?IR=T>
- Camoens, A. (2017, April 10). Klang man arrested for insulting govt leader. The Star Online. Retrieved April 10, 2017 <http://www.thestar.com.my/news/nation/2017/04/10/klang-man-arrested-for-insulting-govt-leader/>
- Centre for Independent Journalism. (2017). Frequently asked questions on section 114A of the Evidence Act 1950, - presumption of fact in publication. Retrieved June 27, 2017 <https://stop114a.files.wordpress.com/2012/08/stop114a-faq-english.pdf>
- Centre for Independent Journalism. (2012). Frequently asked questions on section 114A of the Evidence Act 1950 – presumption of fact in publication. Retrieved June 27, 2017, from <https://stop114a.files.wordpress.com/2012/08/stop114a-faq-english.pdf>
- Ibrahim, M.I. (2017, April 27). Admin WhatsApp boleh dipenjara. Berita Harian. Retrieved July 30, 2017 <https://www.bharian.com.my/node/276393>
- Peters, M. (2012) Malayan Law Journal, 6 MLJ ciii, 1-12
- PP v. Chan Hon Keong* [2012] 5 LNS 184
- PP v. Muslim Ahmad* [2013] 5 CLJ 822
- PP v. Rutinin Suhaimin* [2013] 2 CLJ 427
- Radhakrishna, G. (2013). Current Law Journal, 1 LNS(A) lxxxv, 1-39
- Rutinin Suhaimin v PP* [2015] 3 CLJ 838
- The Sun Daily. (2012, September 18). Section 114A: Thorough investigation still required says AG.
- YB Dato' Hj Husam Hj Musa v Mohd Faisal Rohban Ahmad* [2015] 1 CLJ 787
- Yun, Y. X. (2017, July 2). Man arrested for posting picture insulting PM in WhatsApp group. The Star Online. Retrieved August 30, 2017 <http://www.thestar.com.my/news/nation/2016/07/02/man-arrested-picture-whatsapp>