SEARCH: The Journal of the South East Asia Research Centre for Communication and Humanities Vol. 10 No. 2, 2018, pp. 31-58 ISSN 2229-872X

SOCIAL MEDIA PRIVACY AND THE LAW: PERSPECTIVES FROM MALAYSIAN AND UK CONSUMERS

Jason J Turnerˇ
Taylor's Business School, Faculty of Business and Law, Taylor's University, Malaysia

Puteri Sofia Amirnuddin*
Taylor's Law School, Faculty of Business and Law, Taylor's University, Malaysia

© The Author(s) 2018.

ABSTRACT

The aims of this study are two-fold: firstly to investigate the perspectives of individuals from Malaysia and the UK to understand their views of responsibility and areas of concern about social media in the context of their respective countries and secondly, to examine the role that the law has to play in protecting an individual within the context of social media privacy and the disclosure of personal information. The methodology employed was a convenience sample and google survey with 164 social media users in Malaysia and the UK with supporting evidence provided by follow up interviews with 20 individuals to explore themes that emerge from the quantitative research. The study reveals that the robustness of the law concerning consumer privacy differs between Malaysia and the UK with Malaysia having one Act[1] and the UK having two Acts[2]. However, the varying robustness of the laws protecting consumer privacy on social media had little effect on how an individual views privacy, with the perspectives of respondents being almost identical regardless of the country they lived in. The majority of respondents from both countries indicated it was the responsibility of the 'collective', (the provider, the community, the law and the individual), and not just one stakeholder and/or the legal apparatus to protect a user's privacy online. Respondents felt social media users had to take more responsibility for their privacy and the consequences of any invasion of that privacy with the concept of privacy protection viewed as not just data protection but an all-encompassing phrase which includes how users interact with the platform, the treatment of company and personal information and the rights to access that information. These findings have practical and social implications, which centre on the need for all stakeholders to take 'collective' responsibility for online privacy and the protection of their personal information and for users to be better educated on how they interact with social media. The study should prove useful to consumers and businesses who are already interacting with social media and lawmakers who attempt to enforce the law.

Keywords: Malaysia law; UK law; privacy; personal information; social media

1 The Personal Data Protection Act (2010).

2 The Privacy and Electronic Communications (EC Directive) Regulations (2003) and the Data Protection Act (1998).

ˇCorrespondence email: ***JasonJames.Turner@taylors.edu.my***
*Correspondence email: ***PuteriSofia.Amirnuddin@taylors.edu.my***

1. INTRODUCTION

Social media is not a new phenomenon; it has been in existence since 2002 with the launch of Friendster (Digital Trends, 2016) and was quickly followed by LinkedIn, Myspace, and Facebook. Neither is social media limited to social network websites, rather it includes any form of electronic communication which enables consumers to share information, ideas, messages and other content virtually (Workplace Fairness, 2017; Whitcroft, 2013). Social media platforms have changed and adapted to consumer preferences over time with the underlying popularity continuing to grow, becoming a part of everyday life with the average user spending around 118 minutes every day on social media in 2016 (Statista, 2016).

In January 2016, research conducted by Global Web Index demonstrated that there were 2.307 billion active social media users and 1.968 billion active mobile social users worldwide, which is an increase of 10% and 17% respectively compared to the previous year (Chaffey, 2016). In Malaysia, there are 18 million active social media users, with Facebook the most popular social network platform accounting for over 7 million users, 4 million using Google+, almost 4 million users of Instagram, around 3 million users of Twitter and 2 million users of LinkedIn (Chaffey, 2016). In contrast, there are 38 million active social media users in the UK, with platform usage broadly similar to that of Malaysia with Facebook the dominant platform with almost 18 million users, around 7.5 million users of Twitter, 5 million users of Instagram, around 4 million users of Google+ and LinkedIn, and with 3 million users of Pinterest (Chaffey, 2016; MCMC, 2016; White, 2016).

As the number of social media users increases, the need for regulatory measures and policing over misuse of data and privacy invasions increases in parallel, with individuals concerned about their privacy and the use of their personal data without their consent (Pedley, 2002). These concerns have been reflected in the media over recent years, particularly in the context of the misuse of personal data (Anonymous, 2016a; Dhillon, 2016; Ninomiya, 2016; Teensafe, 2016; Anonymous, 2015; Ozer, 2012; Lewis, n/d) and more recently in terms of cyber-bullying, 'revenge porn' and self-harming (Anonymous, 2017a; Anonymous, 2017b; Anonymous, 2017c; Brown, 2017).

It is in this context, the increased user interaction with social media, where this study will investigate user concerns and perceptions of stakeholder responsibility regarding social media privacy and the treatment of personal information, examining, in particular the role that the law plays in a user's privacy and the protection of their social media information. User's online activities arguably need to be protected by the law and so the law needs to keep up to date with changes in user's online behaviour and the activities of online providers. Using quantitative research and supported by qualitative analysis, the study will address current gaps in the literature concerning privacy and social media, informed consent and whose responsibility it is to protect the information which is disclosed on social media. Through understanding user perspectives and the law, the paper will take research forward in the areas of social media and the law, consolidating existing research in the areas of user privacy and responsibilities for this privacy.

2. LITERATURE REVIEW

Over recent years, there has been an increased use of social media (Weller, 2016; He and Zha, 2014; Tan, *et al*., 2012) for both social interaction, workplace interaction and as platforms to conduct business (Opgenhaffen and Claeys, 2017; Benson, Saridakis and Tennakoon, 2015; Taylor, *et al*., 2015; Adams, 2014; Hugl, 2011). This has led to discussions on how information shared between the users and the provider is appropriated, disclosed, and what constitutes an intrusion on this shared information, in other words, issues of personal information and privacy (Cohen, 2016; Aguirre, *et al*., 2016; Benson, Saridakis and Tennakoon, 2015; Tan, *et al*, 2012; Karniel and Lavie-Dinur, 2012; LexisNexis, 2007; Prosser, 1960). According to Facebook founder, Mark Zuckerberg individuals have become more comfortable with sharing different types of information (Johnson, 2010) and that privacy is largely false (Pierson and Heyman, 2011) and no longer considered a priority for users (Karniel and Lavie-Dinur, 2012). This research contends that the issue of privacy is more complicated than this and indeed rather than no longer being interested in privacy, social media users are in fact even more aware of their privacy and violations of this privacy (Karniel and Lavie-Dinur, 2012) but are not necessarily fully privacy aware.

When the current literature is reviewed, there are a number of themes which have emerged. Firstly, what constitutes privacy and personal information; secondly, whether the user's disclosure of information is informed, making the distinction between user information given freely and that information which is given unwittingly or captured covertly, and finally whose responsibility it is to protect the information which is disclosed on social media (Li, *et al*., 2016; Trottier, 2014). It is argued by Lewis, Kaufman and Christakis (2008) that individuals, particularly young individuals, understand privacy settings and are influenced by friends as well as self-regulation (Steeves and Regan, 2014; Jade, 2012; Hugl, 2011). However, a user's knowledge and understanding of how private their 'shared' information is and with whom this information is being shared is arguably less complete. Social media and online users, particularly younger users, do not seem to understand the privacy trade-off when subscribing to social media platforms (Tan, *et al*., 2012; Milne and Gordon, 1993), and therefore raises the question of who is responsible for this understanding and transparency.

The issue of privacy is often debated and yet it is difficult to find a consistent definition (Tan, *et al*., 2012; Van Lieshout, *et al*., 2011). For the purpose of this research, privacy will be defined as the "information an individual wishes to keep private" (Conger, Pratt and Loch, 2013, p.401) with a distinction made between a user's privacy and right to privacy. It has been argued in the literature that individuals are willing to disclose and share personal details about themselves and in many cases do this voluntarily (Benson, Saridakis and Tennakoon, 2015; Jiang, Heng and Choi, 2013; Phelps, Nowak and Ferrell, 2000). This research will investigate the extent to which this disclosed personal information is indeed considered by the user private and whether the consent given is informed (Noain-Sánchez, 2016; Gratton, 2014; Steeves and Regan, 2014; Hugl, 2011; Onn, 2005). Personal information is argued to include anything from personal descriptors (name, age, place, date of birth, height, weight, hair and eye colour), through to identification numbers (financial, credit and employment information, health and criminal information), education and lifestyle (personality, marital status, comments and opinions), (Anonymous,

2016b). Clearly, some information is more private than others, with individuals having their own unique interpretations of privacy, recently referred to as circles of privacy (Information Commissioner's Office, 2012; Karniel and Lavie-Dinur, 2012). It would be the responsibility of not only the provider but also the user and perhaps other stakeholders in the social media environment to maintain the privacy of this information.

The invasion of a user's privacy can result in any number of negative outcomes such as online bullying, dependency particularly among young adolescents, data and identity theft and reputational damage (Anonymous, 2017a; Anonymous, 2017b; Anonymous, 2017c; Anonymous, 2016a; Brown, 2017; Dhillon, 2016; Ninomiya, 2016; Teensafe, 2016; Anonymous, 2015; Barcelos and Rossi, 2014; Steeves and Regan, 2014; Karniel and Lavie-Dinur, 2012; Lewis, n/d). However, as eluded to earlier, there appear to be two sides to the privacy argument : firstly the privacy which may or may not be violated by a provider or a third party which is a result of the user knowingly disclosing information. Secondly, the privacy which may or may not be violated by the provider or other third party as a result of a lack of the users understanding of the terms and conditions or transparency on the part of the provider. The interaction between the social media user, other users, the provider and the law is complex and requires clarity around transparency, self-determination (Matzner, 2014; Venezia, 2012), perceived privacy, disclosure and the right to control dissemination and use of information (Al-Saggaf, Y, 2017; Benson, Saridakis and Tennakoon, 2015; Malhotra, Kim and Agarwal, 2004; Karniel and Lavie-Dinur, 2012; Pierson and Heyman, 2011; Buchanan, *et al*., 2007). Providing clarity would enable an invasion of privacy to be determined and whose responsibility it is to ensure a user's privacy is protected on social media. Many consumers are not clear about their rights to privacy despite the vast amount of personal information voluntarily disclosed via social media, and they are also not clear about who to contact should they encounter difficulties online and on social media (Trottier, 2014).

Differences and similarities between countries are to be expected (Suzuki and Takemura, 2013) which is why this research has selected two countries to compare user perspectives. Malaysia and the UK were selected for their positions on the social media regulatory spectrum, i.e. the UK being considered relatively advanced in terms of regulatory measures and Malaysia considered to be in the developmental stage of their online and social media regulations. In both Malaysia and the UK, there is no one definitive definition of a 'right to privacy' provided by the case law or statutes (Campbell v MGN Ltd, [2004]; Yong, 2009). However, for the purpose of this paper, we will use the most commonly used definition of 'right to privacy', which is the freedom from interference by other people and organisations (Clarke, 2014). Despite having a general right to privacy, consumers have a tendency to sign away their privacy without having an understanding of the terms and conditions in order to have access to a particular social media. The reasons for users signing away their privacy could be that they trust the provider (Sherchan, Nepal and Paris, 2013) or they simply wish something in return for their information (Li, *et al*., 2016; Rainie and Duggan, 2016; Milne and Gordon, 1993). The ignorance of the consumers on how their consent works could open a gateway for data controllers (UK Data Protection Act 1998, s.1{1}), (UK Government, 1998) or data users (Malaysia Personal Data Protection Act 2010, s.4), (Malaysian Government, 2010) to collect and process consumers'

personal information for various purposes. The extent to which the compilation and processing of consumers' personal information without actual consent amounting to a breach of individual privacy will be debated in the next section.

2.1 The legal perspective in Malaysia

In Malaysia, the right to privacy does not have the same constitutional recognition when compared to other rights stipulated in the Constitution (Yusoff, 2014) with only the Personal Data Protection Act 2010 ('PDPA') legally protecting an individual's privacy and personal information.[3] The PDPA applies to the processing of personal data in commercial transactions and refers to any person who possesses personal information and any person who has control over any personal data in respect of commercial transactions (Malaysian Government, 2010, s.2{1}{a} and {b}). Prior to 2010, an individual could obtain general protection for his/her right to privacy from other legislation such as Penal Code, Communications and Multimedia Act 1998, and Criminal Procedure Code. However, the privacy protection provided by these Acts was general in nature and did not cover access to information without consent.

The PDPA applies only if the person has an establishment in Malaysia and that person is processing, or a representative of the person processing, the personal data (Malaysian Government, 2010, s.2{2} {a} and {b}). The meaning of 'person' in this case is not limited to an individual but it includes an entity incorporated under the Companies Act 1965[4], a partnership, unincorporated association formed under Malaysian law and also to any person having an office in Malaysia (Malaysian Government, 2010, s.2{4}).

The PDPA protects users from having their personal data used without their consent, with personal data or information defined as any information that is processed with respect to commercial transactions by which the information is processed using any equipment that is capable of operating automatically and able to identify the user (Malaysian Government, 2010, s.4). Looking closely into the wording, it can be seen that the definition of 'personal data' applies to the processing of the information based on the instructions given for 'a particular purpose'. The PDPA is non-committal with regard to the definition of 'instructions' whether it is given by the users or by the provider and also the scope of that 'particular purpose.' This indicates that although the PDPA protects the manner in which personal data can be used and processed, it depends on the details of the instructions and the purposes specified in the agreement. The users' personal data will only truly be protected if the clauses in the agreement are more specific and therefore highlights a limitation in the current legal provision in Malaysia.

2.2 The legal perspective in the UK

In the UK, it has been accepted that there is a general right to privacy, although there is no specific legislation that provides this right to privacy. The concept dates back to 1948 where the word 'privacy' appears in Article 12 of the Universal Declaration of Human Rights, and subsequently reflected upon in Article 8 of the Convention for the Protection of Human Rights. The recognition of an individual's right to privacy,

3 There are 9 fundamental liberties highlighted in the Federal Constitution but the right to privacy is not expressly stated as one of these rights.

4 Which has been replaced by Companies Act 2016.

even though the right is not explicit, is embedded in Article 8[5] of the Schedule 1 of the Human Rights Act (HRA) 1998 which provides a right of respect towards an individual's privacy and family life. Prior to the HRA, there was no common law towards an invasion of privacy (Wainwright v Home Office {House of Lords}, 2003). Following the enforcement of the HRA, the privacy protection for individuals was afforded under a breach of confidence but the Act did not provide comprehensive protection for private information (Yusoff, 2014). The limited protection given towards individual privacy gave rise to the Data Protection Act (DPA), 1998. The DPA highlighted the acceptance of the right of individuals to a private domain (Jay, 2000). Although there are various instances where an individual's right to privacy was clearly expressed in the directive, there was no mention of the word 'privacy' in any of the DPA clauses. The DPA was carefully worded, using the phrase 'to regulate' in its clauses instead of 'to protect' personal data or information. This highlights that although the DPA is not intended to be privacy legislation, it affords protection to individual privacy by requiring consent for the processing of personal data (UK Government, 1998, s.4 {3}). However, the effectiveness of this protection is debatable in the complex context of personal data on social media platforms.

The purpose of the DPA is to regulate the processing of information and consists of wide-ranging provision which applies not only to the general aspect of processing but includes obtaining, holding, using and exposing personal information by the data controller for non-domestic purposes (UK Government, 1998, preamble). With regard to the phrase non-domestic purposes, section 36 of the DPA indicates that the data processed is not for the purposes of individuals' personal, family or household affairs (UK Government, 1998, s.36). If the data is considered as 'domestic purposes', that is personal data processed by an individual for their own personal purposes, this data is exempt from the data protection principles (UK Government, 1998, s. 36). It is the duty of a data controller to comply with the data protection principles with regard to all personal data (UK Government, 1998, s.4 {4}) especially when the data controller is established in the UK (UK Government, 1998, s15{1}{a}), with provisions applying to both companies operating offline, online and on social media.

2.3 Application of the law to social media

With a degree of ambiguity and interpretation in the law in both Malaysia and the UK over privacy, what are the consequences for providers? Facebook and other social media providers have experienced controversy recently with incidents over their privacy policies (Anonymous, 2014; Edwards, 2014). The most recent of these was in 2015 when over 600,000 Facebook users unknowingly participated in a psychological experiment organized by Facebook, highlighting issues over privacy and data protection breaches (Williams, 2016; Fishleigh, 2015). As a result of the incident, Facebook was asked to sign an undertaking committing to provide clearer explanation to its users on how their data would be used and to give users ongoing control over the information (Denham, 2016). This has resulted in Facebook and other social media providers frequently updating their policies to ensure that the terms of agreement are in compliance with the regulations (Opsahl, 2010). However, this can create confusion

5 Article 8 of the Human Rights Act (1998) is a broad-ranging right, which includes amongst others, rights to a private life, to individual sexuality, to private and confidential information and to a reasonable expectation of privacy.

with the periodic updating/changing of the terms in the privacy settings making it less not more transparent for users, with confusion over the most recent rights and privacy arrangements (Edwards, 2016).

The privacy settings on a social media platform is not a blanket disclaimer for Facebook or any other social media providers to use personal data as not all users understand the consequences for their personal data following registration. In the introductory paragraph of their terms and conditions, Facebook indicates that the terms of the agreement are subject to periodic change and the continued use of Facebook would be considered an acceptance of the new terms, policies, and guidelines (Facebook, 2017{a}{c}{d}). Furthermore, under Clauses 2(1) and (3) of the Facebook terms and conditions, users permit Facebook to access all content and information as well as their personal data. In the UK, having accepted the new terms and conditions set by Facebook, users are said to have given Facebook and other social media providers who operate in the same way, permission to process personal data in compliance with section 7 of the DPA. However, there is debate as to whether Facebook's use of a users' personal data for purposes other than registration amounts to a breach of privacy and whether the collection of Facebook posts and 'likes' to build advertising profiles could also be a breach of privacy (Edwards, 2016). Although Facebook is allowed to obtain record or hold information, Facebook is bound by section 2 of Schedule 1 Part 1 DPA where it is stated that personal data shall be obtained only for one or more specified and lawful purposes, and shall not be processed in any manner incompatible with the intended purposes. The word 'shall' is given a mandatory effect which means Facebook must not use users' personal information for the purpose other than what was originally intended. Apart from that, section 7(1)(a)(b) and (c) of the DPA[6] ensures users are informed by Facebook whether their personal information is being processed and for what purpose.

This legal discussion from the UK highlights the fact that Facebook does not have an absolute right to use users' personal information despite them having their consent through a user's agreeing to the terms and conditions upon registration for a Facebook account. The Science and Technology Committee (UK Parliamentary Select Committee) has even stated in its report that the acceptance of the terms and conditions upon registration does not amount to a user's informed consent for the provider to use his/her personal information for the purpose other than for registration (Science and Technology Committee, 2014). It was also noted by the Science and Technology Committee (2014) that the terms and conditions are usually printed in small font and are rarely read in detail or understood by users. Even though the DPA is not specific in terms of what information can be obtained and used by social media providers, it does provide online users with a level of protection. Facebook and other social media providers must communicate effectively to users how they intend to use personal information and draw a distinction between information required to access a service and information which they require for other purposes.

6 Data Protection Act 1998, s.7 provides — (1) Subject to the following provisions of this section and to sections 8 and 9, an individual is entitled (a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller, (b) if that is the case, to be given by the data controller a description of— (i) the personal data of which that individual is the data subject, (ii) the purposes for which they are being or are to be processed, and (iii) the recipients or classes of recipients to whom they are or may be disclosed, (c) to have communicated to him or her in an intelligible form— (i) the information constituting any personal data of which that individual is the data subject, and (ii) any information available to the data controller as to the source of those data.

Similar to the UK, users in Malaysia tend to sign away their privacy upon accepting the terms and conditions of a service unless they write to Facebook to waive any of the clauses as required by Clause 18.5 of the Facebook Agreement. The users can write to Facebook explicitly to opt out from any of the clauses, however, the waiver must be signed by Facebook. If a user chooses to write to Facebook because they do not agree to the terms and conditions, Facebook can either waive or sustain the clause(s) leaving the user with access or no access. It should be noted that if Facebook considered waiving adherence to its terms and conditions, this could set a precedent where all users, past and present refuse to agree to the terms and conditions of use yet still be able to access their Facebook account and therefore is considered unlikely. This situation highlights the fact that users have limited opportunities to object to the processing of personal data or information at the stage of registration but can change the privacy settings upon having access to Facebook if they are suitably knowledgeable, as Facebook currently has no legal obligation to inform users about this. It should also be noted that even if the user wishes to customise his/her privacy settings, the scope is limited to the uploading and deleting of posts, visibility of profile page, friend list, likes and comments, tagging and untagging, photos, timeline, searching and newsfeeds (Facebook, 2017c). The collection of personal data[7] will be carried out by Facebook unless the user chooses to preclude Facebook from tracking its online and Web viewing activity (Facebook, 2017{a}{b}{c}{d}).

In Malaysia, Facebook is legally governed by the PDPA (Malaysian Government, 2010, ss. 2{2}{a} and 4). This is because Facebook has a local office in Kuala Lumpur and processes users' data (Leng, 2016). As Facebook is categorised as a medium for commercial transactions, they are required to ensure the user agrees to the terms and conditions, data and cookies policies prior to providing user's access to Facebook (Malaysian Government, 2010). It can be argued that there is a contract present between Facebook and its users as they are providing services in terms of accessibility to a social media platform. However, in order to have an enforceable contract, Facebook is required by law to inform its users of the purpose of collecting personal data[8] prior to users' registration (Malaysian Government, 2010, s.7). Facebook must also inform its users that their personal data will be disclosed to third parties and the identity of the third parties must be revealed to the users (Malaysian Government, 2010, s.8{a} and {b})[9]. It appears that Facebook has been complying with PDPA as it is evident under Clause 9 of the Facebook Agreement that the users are informed of the purposes of data collection which includes: for the use of advertising and with regard to the identity of third parties, found under the 'Advertisement Preferences' section (Facebook, 2017b). In other words, as Facebook allows the user to adjust aspects of their privacy settings, they are now compliant with the law in the UK and Malaysia.

7 For example, collecting information on the types of content its user's view, duration of its users' activities, online payments made via Facebook and activities from third-party services ((Facebook, 2017abcd).

8 *Personal Data Protection Act 2010*, s.7(1) (a) – (h) deals with notice and choice principles, for example: a data user shall provide a written notice to its data subject that his/her personal data is being processed and the purposes of the processing of personal data.

9 *Personal Data Protection Act 2010*, s.8 states that no personal data will be disclosed without the consent of the users. This is subject to *s.39*.

Through the insertion of clauses in the terms and conditions highlighting the possibility of data collection and the risk of uploading personal information online, they are transferring the onus of responsibility to the user who may or not be fully aware of it, yet has been implicitly informed.

As it may be observed from a review of the literature, particularly the legal framework around which social media providers engage with users, there are areas where this research will consolidate existing literature and also take existing research forward. Using the perspectives of Malaysian and UK social media users, this research will address gaps in the current literature particularly in the areas of privacy and social media research, informed consent and to find out whose responsibility it is to protect information which is disclosed on social media. Through understanding user perspectives and understanding of the law, the study will take the literature forward in the areas of social media and the law and how users interpret the role of the law in their right to privacy.

3. METHODOLOGY

In February and March 2017, the study used online interviewer-completed questionnaires with 164 respondents from Malaysia, the UK, and a series of semi-structured interviews with 20 respondents who indicated a willingness to participate in exploring the themes to emerge from the quantitative research. The rationale behind using this approach was two-fold. Firstly, Malaysia and the UK were selected because of fundamental similarities in their legal systems and the use of Law of the Commonwealth , with Malaysia being a colony until 1957. In addition to that, the two countries provide an interesting contrast with the UK being quite advanced in terms of the laws governing privacy and personal data and Malaysia at a relatively early stage of implementing such laws. Secondly, a number of key themes pertaining to users' use of social media and the responsibility of identified stakeholders towards privacy and the disclosure of personal information emerged from the literature which shaped the questions used in the questionnaire. Following statistical testing of the quantitative results using SPSS, the study used qualitative research to explore themes which required to be quantified and interpreted, the results of which were analysed using content analysis.

The study used convenience sampling across two online population sources as this was considered the most appropriate approach to access a diverse range of social media users from Malaysia and the UK. It is acknowledged, however, that the approach carries the limitation that only those respondents able or willing to complete the survey during the four-week period did so (Collis and Hussey, 2014). A further limitation of this study was the sample size, which although appropriate for exploratory research into respondent perspectives of social media, would have benefitted from being larger and perhaps incorporating the use of quota sampling to better ensure "that the overall sample has the same characteristics as the population" (Waters, 1998, p.78) and through using an interlocked design (Kent, 1999) further explore differences between populations on the basis of country of origin, age, and gender. However, given that responses from both UK and Malaysian respondents were almost identical; this was not deemed a major limitation on the research findings, rather a consideration for future research.

To ensure the questions in the questionnaire were understandable the research conducted a pilot study with 10 respondents, the results of which confirmed that questions were unambiguous, with the appropriate balance of question type and number of questions. With regard to the internal consistency of the online questionnaire, a Cronbach's Alpha coefficient was used (the test revealed a figure of 0.819) which represents a good scale and valid test model (Malhotra and Birks, 2006)

4. ANALYSIS AND DISCUSSION

Prior to analysing social media usage, respondents were asked a series of questions relating to their demographics. With regard to the quantitative component, 42.1% were males and 57.9% were females with 50% aged 21 and under, 39.6% aged 22–40, 8.5% aged 41–60 and 1.8% aged 61 and over. With regard to the respondents' country of origin, 73.8% came from Malaysia and 26.2% came from the UK. With regard to the qualitative component, respondents were evenly divided between male and female and were aged between 22 and 57, with the majority aged 28 years and over. In terms of country of origin, 50% of respondents came from Malaysia and 50% came from the UK. Such figures are broadly representative of the social media using population in Malaysia and the UK (MCMC, 2016; White, 2016).

4.1 Social media use and usage

As respondents for the qualitative research came from the original quantitative research and were asked questions on social media use and usage as part of the quantitative research, the findings in this section apply to the 164 respondents. The majority of respondents had been using social media for over four years, using it daily with no difference between Malaysian and UK respondents. A total of 95.1% had been using social media for 4 years or more, 3.7% had been using social media for between 2 and 4 years and only 0.6% of respondents had been using social media for between 1 and 2 years and for less than 1 year. Use of social media was predominantly daily (90.9%), with 5.5% using social media between 4 and 6 times and 1.8% either using social media 2 to 3 times a week or once a week which is supported by the literature (Statista, 2016).

The most popular platforms for respondents to use were Facebook, YouTube, and Instagram, which is in line with existing research (Chaffey, 2016; Statista, 2016) with the majority of respondents from Malaysia and the UK selecting a minimum of 2 platforms as can be seen from **Table 1** below.

Table 1. Social media platforms used by respondents on a regular basis

Platform	Number of responses	Percentage
Facebook	149 responses	90.9%
YouTube	141 responses	86%
Instagram	122 responses	74.4%
Twitter	71 responses	43.3%
LinkedIn	43 responses	26.2%
Pinterest	32 responses	19.5%
Tumblr	22 responses	13.4%

In investigating Malaysian and UK respondents' reasons for using social media in **Table 2,** the most popular motives were 'for entertainment', 'chatting with others' and 'keeping up-to-date with current events' which is also in line with existing research (Chaffey, 2016; Adams, 2014). It was revealed that respondents do not use social media for one particular reason and can easily multitask and exhibit cross-platform behaviour, i.e. use social media platforms to perform different tasks simultaneously. The predominant platform used was Facebook with YouTube accessed in many cases through Facebook with respondents not leaving the Facebook platform to satisfy their needs; a typical response from respondents was "I use social media to scroll through Facebook to see what's happening, post messages, chat to friends and click on links to YouTube". These results inform the research that the majority of respondents from both Malaysia and the UK have been using social media for over 4 years on a daily basis, particularly the platforms Facebook, YouTube, and Instagram, with Facebook the main platform used to simultaneously socialise with friends, keep up-to-date with events and be entertained. Regardless of country of residence, respondents exhibited almost identical characteristics which indicate that Malaysian and UK respondents use social media in the same way which is perhaps unsurprising. The research also demonstrates that the respondents are familiar, have experience with social media, and are therefore able to provide informed opinions on questions relating to the research, providing reassurance, to a degree, of the validity of the responses.

Table 2. Reasons for social media use by respondents on a regular basis

Reason for social media use	Number of responses	Percentage
For entertainment	151	92.1%
Keeping up to date with current events	134	81.7%
Chatting with others	133	81.1%
Product and service research	81	49.4%
To get reviews and recommendations	70	42.7%
Others (not specified)	14	8.5%

4.2 Privacy and Personal information

As indicated in the previous section, for this part of the study, respondents for the qualitative research came from the original quantitative research and were asked open questions relating to privacy and personal information as part of the quantitative research, and therefore the findings relate to 164 respondents. Respondents were asked to define privacy and personal information. It was considered important to the validity of the research to ensure respondents understood concepts which they were later going to be asked about in the context of their perceptions, concerns and who they felt was responsible for privacy and personal information on social media. With regard to the definitions of privacy, there were no commonalities of responses, although it should be noted that the majority of respondents from Malaysia and the UK considered privacy and personal information as inter-related, i.e. a respondent's privacy was related to the protection of his/her personal information, which is discussed in the literature

(LexisNexis, 2007). There was no difference between responses from Malaysian and UK respondents. Following a content analysis of the findings, the three main themes revealed from the definitions of privacy were: respondents thought it implied informed consent; user control over personal information; and the responsibility of the provider to protect a user's privacy. Typical responses were "I need to know that strangers cannot view my posts and photos without my expressed consent"; "having full control over who can and cannot see/obtain your information"; "your personal information should be protected, chats with friends should be encrypted, voice or video calls should also be protected from hacking. Personal activity on sites should not be tracked and if cookies need to be used, there should be a warning beforehand". What these responses reveal is that not only did respondents understand what privacy meant, they were concerned with privacy and its link to a range of personal information and online behaviour and thought their personal information should be protected. Later in the paper, respondents' concerns with and responsibilities for social media privacy and personal information will be examined, investigating further these findings and those found in previous research (Benson, Saridakis and Tennakoon, 2015; Steeves and Regan, 2014; Tan *et al*., 2012; Hugl, 2011).

With regard to personal information, the majority of respondents from Malaysia and the UK considered this to mean, as one respondent put it, "anything beyond name/sex/age" which is supported by the literature (Anonymous, 2016b; Gratton, 2014). Respondents considered financial, residential, legal and medical information as 'personal' and not information they would readily reveal on social media, with a typical response being "any information that would influence my life if it is misused…i.e. financial, legal medical and also private residential information, addresses, phone number and email address". A minority of respondents from the UK considered personal information to also include material relating to their child or children with a typical response being "my home address, where I [am] located, credit card details and where my kids [go] to school". In other words, respondents considered personal information that which uniquely identified them which corresponds to the definitions in the literature (Anonymous, 2016b; Gratton, 2014; Information Commissioner's Office, 2012). Having had almost identical responses to questions, it should be noted that responses to this question differed slightly between those respondents from Malaysia and the UK with a minority of respondents from the UK being of the opinion that personal information included information pertaining to children, not one respondent from Malaysia mentioned children in the context of personal information. The qualitative research was unable to explain this finding beyond respondents simply indicating the factors which first came to mind. It may be nothing more than an interesting aside, however in a subsequent study this will be investigated further to see how parents and children view social media and their privacy on platforms such as Facebook.

4.3 Invasion of privacy

Having established respondents' understanding of privacy and prior to examining respondent perceptions of social media privacy and personal information, respondents were asked if they themselves had experienced or known of anyone who had experienced having their privacy invaded on social media. As indicated in the previous section, for this part of the study, respondents from the qualitative research

came from the original quantitative research and were asked this question as part of the quantitative research and therefore the findings on invasion of privacy apply to the 164 respondents. Although Malaysian and UK respondents were rather evenly divided in terms of agreement and strong agreement (37.8%), neutrality (33.5%) and disagreement and strong disagreement (28.7%) over whether they themselves had experienced their privacy being invaded, a total of 75% agreed and strongly agreed, 14.6% were neutral and 10.3% disagreed and strongly disagreed that they knew of someone who had experienced an invasion of their social media privacy. This invasion of privacy took the form of hacking, the setting up of a fake account or principally identity theft with typical responses being: "my friend's account got hacked and his info got leaked"; "I've had friends who have had their photographs stolen and then people have duplicated them and made fake accounts using their information and photos"; "I've known people to have their profiles duplicated, their friends to be added, essentially their [online] identity stolen". A minority of Malaysian respondents mentioned cyberbullying with a typical response being "bullying, posting ugly photos online". A minority of Malaysian and UK respondents also cited cyber-stalking with a typical response being "a stalker managed to retrieve personal information of my friend". Such themes are supported by the literature (Brown, 2017; Anonymous, 2016a; Dhillon, 2016; Ninomiya, 2016; Teensafe, 2016; Anonymous, 2015; Lewis, n/d) and provide initial insight into the widespread nature of privacy violations on social media centring on identity replication and theft.

When respondents were asked what action was taken in response to these violations, there was no commonality in the responses but an underlying theme of self-monitoring and awareness were present in the majority of responses which is supported by the literature (Steeves and Regan, 2014; Jade, 2012; Hugl, 2011). The respondents who indicated personal intervention mentioned changing profile passwords, deleting offending posts and reducing social media activity and with typical responses being "change passwords", "delete the post", "change my settings and reduce the time spent on social media". A minority of respondents from both Malaysia and the UK indicated they would contact the police with a typical response being "I would complete a police report" and a minority from Malaysia indicated they would contact the social media platform administrator, with a typical response being "I would contact the administrator first". In ensuring the most satisfactory outcome, the majority of respondents from Malaysia and the UK felt personal intervention was the most appropriate and effective approach to dealing with privacy violation with a typical response being "if you do it yourself its done there and then". When respondents were asked whether they considered involving the law to solve the privacy issue, the response was practically the same between 'yes' (49%) and 'no' (51%), which supports the earlier comments that respondents would first consider personal intervention followed by police or social media administrator intervention (Steeves and Regan, 2014; Trottier, 2014; Jade, 2012; Hugl, 2011). Interestingly, despite the relatively widespread violations of a user's privacy, respondents did not even consider involving the law, even when prompted by the question 'Did you or someone you know consider the law as a means to solve the invasion of privacy on social media?', respondents were divided on involving the law. The reason is the majority of respondents would prefer to solve issues relating to invasions of privacy by themselves as they want the issue dealt with quickly and, as will be revealed later in the research, the majority of respondents lacked knowledge of the laws pertaining to social media and issues of privacy and personal information.

4.4 Disclosure and concerns relating to social media engagement – quantitative findings

Following on from respondents' definitions of privacy and personal information, participants in the quantitative study were asked what information they would be willing to disclose on social media, what information they would not and what information they would be willing to disclose if they had assurances the information would be protected. As it can be observed from **Table 3**, and supported by the earlier discussion, it is clear where the users' boundaries are when it comes to the particular information respondents are willing to disclose. Respondents from Malaysia and the UK appeared to share information regarding business address, date of birth, current employment and employment history as well as personal interests. The reasons for this are presumably that such pieces of personal information are some of the standard requirements for registering on social media platforms (Anonymous, 2016b; Clarke, 2014; Information Commissioner's Office, 2012). In contrast, and as illustrated earlier, respondents from both Malaysia and the UK were less inclined to reveal more personal information such as family information, residential and salary information, medical information and bank and financial information. Such findings are perhaps unsurprising, and maybe so too is the fact that when respondents were prompted to indicate the personal information they would be willing to disclose if they had assurances from the social media provider, there were only small increases in the percentage of those willing to disclose more information in the areas of family information, home address, salary, medical information and banking and financial information.

Table 3. Personal information which respondents would be willing to disclose on social media

Personal information	Willing to disclose percentage	Not willing to disclose percentage	Willing to disclose with assurances percentage
Family information	8.5%	84.1%	22.6%
Home address	3%	93.3%	21.3%
Business address	29.7%	40.2%	31.7%
Bank and financial information	1.8%	95.1%	7.3%
Date of birth	76.8%	17.1%	71.3%
Salary	4.9%	86%	15.2%
Current employment and employment history	47.6%	40.2%	50.6%
Medical information	8.5%	82.9%	15.2%
Personal interests	82.3%	16.5%	69.5%

4.5 Disclosure and concerns relating to social media engagement – qualitative findings

When respondents in the qualitative study were asked to explain why they may be more willing to disclose further personal information if they had assurances from the social media provider, the majority indicated that the reasons were two-fold. Firstly, as they became more comfortable with the social media platform, they were more likely to disclose more information about themselves. Secondly, the trust they had built up over time in the provider gave them more confidence that their personal information would be less susceptible to hacking, theft and misuse, a typical response being: "the longer you are on a social media site you get more confidence with the site and the people so it's only natural you give away a little more information about yourself". It should be noted that respondents from the UK were marginally more likely to reveal more personal information about themselves if they had assurances and trusted the social media provider when compared to their Malaysian counterparts, the reason for this was related to the level of comfort and trust users had with the provider with Malaysian users less trusting of how the information would be used.

The issue of trust in the social media provider is supported by the literature (Sherchan, Nepal and Paris, 2013) and the quantitative study with 60.9% of respondents from Malaysia and the UK agreeing or strongly agreeing with the statement 'using a social media platform I trust reassures me about my privacy', 23.8% of respondents being neutral and 15.3% disagreeing or strongly disagreeing. Similarly, the majority of respondents (with no significant difference in the responses from Malaysian and UK respondents) agreed or strongly agreed (75%) that they were more likely to trust a social media provider who discloses how they intend to use a respondents' information, with 15.9% of respondents neutral and 9.1% disagreeing or strongly disagreeing. Trust or as it has been termed in the literature 'social trust' in the social network as well as the provider are important ingredients to the disclosure of information (Sherchan, Nepal and Paris, 2013) and can help in the alleviation of concern relating to an individual's social media activity. The extent to which respondents were concerned and what they were concerned about in the context of social media privacy and disclosure of personal information will be examined in the next section.

4.6 Concerns relating to social media privacy and personal information – quantitative findings

Respondents were asked to indicate their levels of agreement to questions relating to concerns over their social media activity. As it can be seen from **Table 4**, there were particularly high levels of agreement and strong agreement to questions relating to concern about privacy, security of personal information, monitoring, data theft, hacking and misuse of information with no significant difference between the responses from Malaysian and UK respondents. Of the variables age, gender, country, frequency of social media use and how long respondents have used social media, which were tested for significance using multiple regression, none proved significant.

Table 4. Statistics relating to respondents' concern over their social media activity

Question	Percentage of those who Strongly agreed/ agreed	Percentage of those who were neutral	Percentage of those who Strongly disagreed/ disagreed
I am concerned about my privacy on social media	87.2%	9.8%	3%
I am concerned about the security of my personal information on social media	92.1%	4.9%	3%
I am concerned that someone can monitor my social media activity	85.3%	8.5%	6.1%
I am concerned someone could steal my personal information via social media	92.7%	5.5%	1.8%
I am concerned someone could hack my social media account(s)	94%	3%	3%
I am concerned that someone will misuse the information I give them on social media	88.4%	6.7%	4.9%
I do not know how my information will be used via social media	76.3%	12.8%	10.9%

The particularly high levels of agreement and strong agreement to questions relating to concern over respondents social media activity echo respondents' earlier comments regarding invasions of privacy online and the subsequent theft of personal information, and are key concerns highlighted in the literature (Anonymous, 2016a; Dhillon, 2016; Ninomiya, 2016; Teensafe, 2016; Anonymous, 2015; Lewis, n/d). Respondents were concerned about their privacy, security and the misuse of their information, with the majority being not clear how their information will be used. It is with regard to the latter point, which is particularly concerning, and as we will observe later in the paper is linked to a user's lack of understanding of the terms and conditions and the law which is meant to protect their information. Interestingly enough, concern does not equate to reduced social media use with the majority of respondents in the qualitative research indicating that they would likely use social media more in the future.

4.7 Concerns relating to social media privacy and personal information – qualitative findings

Respondents from the qualitative research were concerned about their social media privacy and personal information, highlighting issues of hacking, security and identity theft with a typical response being "I'm concerned about my privacy, you hear

of accounts getting hacked, of passwords being stolen and people's identities being copied, you have to be careful about the security of your personal information". This typical response supports the levels of strong agreement in the quantitative research and by existing research (Dhillon, 2016; Ninomiya, 2016; Teensafe, 2016; Anonymous, 2015; Lewis, n/d), clearly underlining the fact that more needs to be done to reassure social media users on the safety of their personal information. The need for improved security is particularly important given the fact that the majority of respondents in the qualitative study indicated that their use of social media would increase in the future.

The findings inform the study that although respondents engage regularly with social media, to the extent that the majority of respondents from Malaysia and the UK indicated that they felt that use of social media was becoming an essential part of everyday life and would be used more often in the future, respondents still were concerned about using social media and the information they disclose. Typical responses were "it is indeed part of everyday life as can be observed from the way the handphones become an indispensable fixture" and "most likely using more social [media] in the future". It should be noted, however, that a minority of respondents from Malaysia indicated that they could potentially use less social media platforms in the future, responding "I will cut it into two". The reasons those individuals gave were that the handphone was becoming addictive and had taken up too much of their life. Interestingly, and as mentioned earlier, Facebook is clearly the dominant platform, with respondents using this to do a variety of tasks and even accessing other platforms such as YouTube, hence making it easier to reduce engagement with the number of social media platforms but not necessarily the amount of engagement time.

4.8 Responsibility for social media privacy – quantitative research

The research reveals that respondents were concerned about their social media privacy but who do they think is responsible for their privacy? As it can be seen from **Table 5**, there was relatively high levels of agreement and strong agreement to questions relating to all stakeholders, implying that respondents felt the responsibility for their social media privacy lay with the individual, the provider, the law and to a lesser extent the community, in other words, a collective effort from ~~the~~ all stakeholders (Jade, 2012; Ozer, 2012). Similar to previous responses to questions, there was no significant difference between the responses from Malaysian and UK respondents, with almost identical levels of agreement and disagreement between the two groups of respondents. Of the variables age, gender, country, frequency of social media use and how long respondents have used social media, which were tested for significance using multiple regression, only age and gender proved significant.

Table 5. Statistics relating to who respondents consider responsible for social media privacy

Question	Percentage of those who Strongly agreed/ agreed	Percentage of those who were neutral	Percentage of those who Strongly disagreed/ disagreed	Significant variables
I always read the terms & conditions associated to any social media activity	17.7%	25.3%	67%	Gender $p<.009$
I feel the responsibility for social media privacy rests with the individual user	74.2%	16.5%	10.3%	None
I feel the responsibility for social media privacy rests with the provider	79.9%	14%	6.1%	None
I feel the responsibility for social media privacy rests with the law	72.6%	18.9%	8.5%	None
I feel the responsibility for social media privacy rests with the community (multiple users policing each other and themselves)	65.3%	22.6%	9.4%	Age $p<.001$
I feel the responsibility for social media privacy rests with the individual, the provider, the law and the community	82.3%	13.4%	4.2%	None

Respondents from Malaysia and the UK felt it was the responsibility of all stakeholders to protect their social media privacy, underlined by the strong level of agreement and strong agreement (82.3%) to the question 'I feel responsibility for social media privacy rests with the individual, the provider, the law and the community' which is supported by the literature (Jade, 2012; Ozer, 2012). When the study examines the findings further, it is observed that respondents felt it was the particular responsibility of the provider, the individual and the law which corresponds to the earlier comments related to whom respondents would contact in the event of an invasion of privacy.

4.9 Responsibility for social media privacy – qualitative research

The findings from the quantitative research are supported by the qualitative research with the majority of respondents from Malaysia and the UK of the opinion that it is responsibility of the collective with a typical response being "I think we all share in the responsibility of protecting ourselves and others online. But the government, regulator and law enforcement bodies should also have the primary responsibility to ensure internet services aren't built without proper safety, security and privacy".

A minority of respondents from both Malaysia and the UK emphasised the individual in this collective responsibility with a typical response being "Partially yourself. The other part should be the social media outlet. Facebook has all our personal details so they should bear the responsibility of keeping it secure. But as users, we have to exercise caution when using social media and restraint in putting too much information online".

It is with regard to the individual and their self-regulating of their social media privacy that there appears to be an anomaly with the minority (17.7%) of respondents from the quantitative research agreeing and strongly agreeing that they always read the terms and conditions associated to the social media platforms they engage with. Despite being concerned about hacking, identity fraud and data misuse and feeling they had a personal responsibility for their social media privacy, the majority of respondents from both the quantitative and qualitative studies failed to read the terms and conditions of social media platforms not only prior to subscribing but also with regard to the updates and provider disclaimers. This is a particular issue when we consider that social media providers like Facebook, through the insertion of clauses in the terms and conditions, highlighting the possibility of data collection and the risk of uploading personal information online, are transferring the onus of responsibility to the user who may or may not be fully aware yet has been implicitly informed. The majority of respondents from both Malaysia and the UK in the qualitative study blamed the length of the terms and conditions as the reason for their failure to read, with a typical response being "it's tricky and most of the time it is extremely lengthy. Sometimes I just choose to click on the button without reading the full terms". The literature supports this finding, arguing that the majority of online users rarely or never check their privacy and security settings (Science and Technology Committee, 2014; Adams, 2014; Jade, 2012) unless, as acknowledged by a number of respondents, there had been an invasion of privacy which prompted, as one respondent put it, "after the incident they changed, setting the privacy settings to private". However, as it was noted earlier, users only have scope to change the settings with regard to the uploading and deleting of posts, visibility of profile page, friend list, likes and comments, tagging and untagging, photos, timeline, searching and newsfeeds (Facebook, 2017c) and therefore is not particularly effective.

4.10 The role of the law in protecting privacy and personal information on social media – quantitative research

The majority of respondents were cautious about the personal information they disclosed on social media, had concerns over their privacy and personal information on social media but did not read the terms and conditions and would only appear to take action with their privacy settings when their privacy was invaded (Science and Technology Committee, 2014; Adams, 2014; Jade, 2012). It is the lack of knowledge of the relationship or contract respondents were getting into with their social media provider, which the study will investigate further, addressing the second aim of the research, namely examining the role that the law has to play in protecting a consumer's privacy within the context of social media. No respondent from either the quantitative or qualitative studies explicitly mentioned that they would involve the law following an invasion of privacy (Venezia, 2012) and only 49% of respondents from the quantitative study said 'yes', they or someone else had considered the law when

asked the direct question 'Did you or someone you know consider the law as a means to solve the invasion of privacy on social media?'. Was this lack of consideration of the law in instances of privacy invasion the result of a lack of knowledge of the law? To address this question and the second aim of the study, respondents were asked to indicate their level of knowledge of the law and whether the law should do more to protect both the privacy and personal information of social media users. Respondents were also asked whether they thought the current law needed to be strengthened. As it can be seen from **Table 6**, there were relatively high levels of agreement and strong agreement to questions relating to the role of the law, although it should be noted that the majority of respondents acknowledged that they did not have particularly sound knowledge of the law. Similar to previous comments pertaining to concern over social media activity and responsibility for social media privacy, there was no significant difference between the responses from Malaysian and UK respondents. Of the variables age, gender, country, frequency of social media use and how long respondents have used social media, which were tested for significance using multiple regression, only age and gender proved significant.

Table 6. Statistics relating to the role of law in protecting users of social media

Question	Percentage of those who Strongly agreed/ agreed	Percentage of those who were neutral	Percentage of those who Strongly disagreed/ disagreed	Significant variables
I am aware that there is a law protecting my privacy and personal information on social media	68.3%	17.7%	14%	Gender $p<.001$ Time using social media $p<.001$
I have sound knowledge of the law protecting my privacy and personal information on social media	38.4%	24.4%	37.2%	Country $p<.001$
I feel the law should do more to protect the privacy of social media users	77.4%	18.9%	3.6%	None
I feel the law should do more to protect the personal information of social media users	82.3%	14%	3.6%	None
I feel the current laws affecting privacy and personal information for social media users need to be strengthened	76.2%	20.1%	3.7%	None

The majority of respondents were aware of the respective laws relating to privacy and personal information with 68.3% agreeing and strongly agreeing but did not have sound knowledge (only 38.4% agreeing and strongly agreeing) of the law which raises issues around informed consent and links to the earlier discussion regarding Facebook transferring the onus of responsibility to the user who may or not be fully aware yet has been implicitly informed. What is interesting is that the majority of respondents feel the law should do more to protect users' privacy and personal information but do not have a sound knowledge of the existing laws and do not read the terms and conditions currently available as a result of the law.

4.11 The role of law in protecting privacy and personal information on social media – qualitative research

The lack of knowledge and understanding of the law governing privacy and personal information revealed in the quantitative research is supported by the qualitative study which investigated levels of understanding of the laws protecting user rights on social media. The majority of respondents from Malaysia and the UK indicated they had basic understanding of the law with a typical response being "nothing more or less, my understanding on the PDPA is that it protects personal data from being misused". A minority from Malaysia had a little more knowledge with a typical response being "invasion of privacy, use of personal images for pornography, cybercrime. But in Malaysia, the laws seem to be more of prosecutive in nature". Respondents from the UK had little or no understanding of the law protecting user rights and social media privacy with a typical response being "I have no idea", even when prompted to elaborate on their response, they were unable to provide insight even into the name of the relevant Act.

In the qualitative study respondents were asked to suggest legal measures which they felt could protect the rights of individuals using social media. The key theme to emerge was transparency, with respondents suggesting there was a need to improve awareness, with typical responses being "users have to be clear what they are signing up for, it's a contract after all. Maybe the law could encourage providers to have a shorter terms and condition with users unable to access the digital platform without more than simply an acknowledgement that they had read the material" and "there needs to be a clear definition of what personal data is". A minority of respondents from Malaysia felt the law could impose stricter sentences on offenders with a typical response being "having a legislation which protects the rights is one thing, the enforcement of the legislation is another thing. There is no proper enforcement in place". Such findings indicate that respondents feel the law could do more to encourage transparency and understanding of the law and the wider issue of understanding the implications of using social media, which is a common theme to emerge from this research. However, the majority of respondents do not read the terms and conditions and therefore increased legislation might not be the answer. Rather increased personal responsibility prior to and during engagement rather than after an invasion of privacy is what is required with providers also taking responsibility to be clear in their intentions for use of personal information and not simply operating a policy of caveat emptor.

5. CONCLUSION

Respondents from Malaysia and the UK exhibited almost paralleled responses when it came to their use and usage of social media, concerns with regard to social media, responsibility for privacy and personal information and the role the law plays in protecting a user's privacy and personal information. The similarity in responses can be explained by the fact that social media users consume the services in a similar way and have comparable experiences given platforms such as Facebook operate in the same way in both countries. The research also reveals the contradictory nature of respondents: they understood what privacy meant, they engaged in self-regulation when it came to disclosing personal information and were concerned about their social media security, the potential of theft, hacking and misuse of their personal information. However, the majority of respondents did not read terms and conditions, and did not have a solid knowledge of laws governing privacy and personal information and despite this lack of knowledge, many intended to increase their use of social media. Respondents acknowledged that they themselves could be better informed about the law and be better acquainted and engaged with the terms and conditions of providers they register with but felt it was the responsibility of the 'collective' to ensure user privacy and personal information is protected on social media. Despite complying with the data protection and privacy laws in Malaysia and the UK, respondents felt providers and the law could do more to ensure respondents understood their rights and address the issue of explicit awareness of terms and conditions and their implications. Currently, social media providers like Facebook transfer the responsibility to the user in respect of knowledge of how their personal information will be used and the lack of engagement with the terms and conditions from the user makes additional laws arguably a moot point.

This research has revealed that perhaps new legislation is not the answer rather users need to be 'educated' with regard to their social media responsibilities, and providers need to take more ownership of users' online activities which is an area Facebook is working on with regard to its anti-bullying campaign (Anonymous, 2017a). This 'education' should not be limited to the individual responsibility but as a collective online community, mutually responsible for 'policing' violations of privacy and encouraging more transparency and reducing the number of data thefts, hacking and misuse of their personal information. This is one area for future research to examine ways in which users can be better educated in areas of privacy violations, particularly in light of recent trends in cyber-bullying, 'revenge porn' and self-harming (Anonymous, 2017a; Anonymous, 2017b; Anonymous, 2017c; Brown, 2017). A second area for future research is to investigate and contrast the perspectives from a variety of stakeholders: lawyers, social media providers, police officers and users (including parents and children) to gain a more holistic perspective of privacy responsibility and addressing the negative aspects associated to social media communication. A third area for future research would be to gain further user insight into online user behaviour. Using an online diary or participant observation, research could get 'live' insight into the emotions users go through when dealing with privacy and personal information issues as well, as how users perceive and handle the terms and conditions and updates of these agreements. Such insight will inform the 'education' aspect of future research and take research forward in terms of social media responsibilities and the role of the law.

Open Access: This article is distributed under the terms of the Creative Commons Attribution License (CC-BY 4.0) which permits any use, distribution and reproduction in any medium, provided the original author(s) and the source are credited.

REFERENCES

Adams, A. A. (2014). Facebook code: Social network sites platform affordances and privacy. *Journal of Law, Information and Science*, *23*(1), 158-168.

Aguirre, E., Roggeveen, A.L., Grewal, D., & Wetzels, M. (2016). The personalization-privacy paradox: Implications for new media. *Journal of Consumer Marketing*, *33*(2), 98-110.

Al-Saggaf, Y. (2017). Information sharing on Facebook by Alone, Single and Lonely Female Users. *SEARCH: The Journal of the South East Asia Research Centre for Communications and Humanities, 9*(1), 97-116.

Anonymous. (2014). Facebook faces UK probe over emotion study. *BBC News*. Retrieved from: http://www.bbc.com/news/technology-28102550.

Anonymous. (2015). Cyberbullying and social media. *Megan Meier Foundation*. Retrieved from: http://www.meganmeierfoundation.org/cyberbullying-social-media.html.

Anonymous. (2016a). Identity fraud up by 57% as thieves 'hunt' on social media. *BBC News*. Retrieved from: http://www.bbc.com/news/uk-36701297.

Anonymous. (2016b). Personal information. *PrivacySense.net*. Retrieved from: http://www.privacysense.net/terms/personal-information/.

Anonymous. (2017a). Facebook to train teens as anti-bullying ambassadors. *Skynews*. Retrieved from: http://news.sky.com/story/facebook-to-train-teens-as-anti-bullying-ambassadors-11083573.

Anonymous. (2017b). Australia launches website to report revenge porn in 'world first'. *Skynews*. Retrieved from: http://news.sky.com/story/australia-launches-website-to-report-revenge-porn-in-world-first-11084799.

Anonymous. (2017c). Social media blamed for bug rise in girls self-harming. *Skynews*. Retrieved from: http://news.sky.com/story/social-media-blamed-for-big-rise-in-girls-self-harming-11087346.

Barcelos, R. H., & Rossi, C. A. V. (2014). Paradoxes and strategies of social media consumption among adolescents. *Young Consumers*, *15*(4), 275-295.

Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users: Does control over personal information, user awareness and security notices matter? *Information Technology & People*, *28*(3), 426-441.

Brown, V. (2017). Cyberbullying: Words can hurt too. *The Star Online.* Retrieved from: http://www.thestar.com.my/news/nation/2017/10/19/cyberbullying-words-can-hurt-too/.

Buchanan, T., Paine, C., Joinson, A.N., & Reips, U.D. (2007). Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 157-165.

Campbell v MGN Ltd [2004] UKHL 22 at para 11 per Lord Nicholls of Birkenhead.

Chaffey, D. (2016). Global social media research summary 2016. *Smart Insights*. Retrieved from: http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/.

Clarke, R. (2014). Privacy and social media: An analytical framework. *Journal of Law, Information and Science*, *23*(1), 169.

Cohen, S. (2016). Privacy risk with social media. *The Huffington Post*. Retrieved from:http://www.huffingtonpost.com/sam-cohen/privacy-risk-with-social-_b_13006700.html.

Collis, J., & Hussey, R. (2014). *Business research: A practical guide for undergraduate and postgraduate Students (4th Ed)*. New York: Palgrave.

Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal*, *23*(5), 401-417.

Denham, E. (2016). Information commissioner updates on WhatsApp/Facebook investigation. *Information Commissioner's Office blog*. Retrieved from: https://iconewsblog.wordpress.com/2016/11/07/information-commissioner-updates-on-whatsapp-facebook-investigation/.

Dhillon, R. (2016). Social media monitoring an invasion of privacy, says Empower. *The Rakyat Post*. Retrieved from: http://www.therakyatpost.com/news/2016/01/12/social-media-monitoring-an-invasion-of-privacy-says-empower/.

Digital Trends. (2016). The history of social networking. *Digital Trends*. Retrieved from: http://www.digitaltrends.com/features/the-history-of-social-networking/.

Edwards, J. (2014). Facebook faces government probe over study that manipulated users' emotions without telling them. *Business Insider*. Retrieved from: http://www.businessinsider.my/facebook-faces-probe-over-emotion-manipulation-study-2014-7/?r=US&IR=T#U6arFjPgVclmpeUL.97.

Edwards, L. (2016). Privacy in public spaces: What expectations of privacy do we have in social media intelligence? *International Journal Law and Information Technology*, *24*(3), 309.

Facebook. (2017a). Data policy. *Facebook*. Retrieved from: https://en-gb.facebook.com/about/privacy/.

Facebook. (2017b). How does Facebook decide which ads to show me and how can I control the ads I see? *Facebook*. Retrieved from: https://en-gb.facebook.com/help/562973647153813/.

Facebook. (2017c). Manage your privacy. *Facebook*. Retrieved from: https://en-gb.facebook.com/about/basics/manage-your-privacy.

Facebook. (2017d). Statement of rights and responsibilities. *Facebook*. Retrieved from: https://en-gb.facebook.com/legal/terms.

Fishleigh, J. (2015). Is someone watching you? Data privacy and protection: Current issues. *Legal Information Management*, *15*, 61.

Gratton, E. (2014). If personal information is privacy's gatekeeper, then risk of harm is the key: A proposed method for determining what counts as personal information", *Alb. L. J. Sci. & Tech*, *24*, 205-209.

He, W., & Zha, S. (2014). Insights into the adoption of social media mashups. *Internet Research*, *24*(2), 160-180.

Hugl, U. (2011). Reviewing person's value of privacy of online social networking. *Internet Research*, *21*(4), 384-407.

Information Commissioner's Office. (2012). Determining what is personal data. *ICO*. Retrieved from: https://ico.org.uk/media/1554/determining-what-is-personal-data.pdf.

Jade, A. (2012). Personal responsibility over your online privacy. *The Online Image*. Retrieved from: http://theonlineimage.weebly.com/.

Jay, R. (2000). UK Data Protection Act 1998 – The human rights context. *International Review of Law Computers*, *14*(3), 385.

Jiang, Z. J., Heng, C. S., & Choi, B. C. (2013). Research note-privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research*, *24*(3), 579-595.

Johnson, B. (2010, January 11). Privacy no longer a social norm, says Facebook founder. *The Guardian*, n/p.

Karniel, Y. & Lavie-Dinur, A. (2012). Privacy in new media in Israel. How social networks are helping to shape the perception of privacy in Israeli society. *Journal of Information, Communication and Ethics in Society*, *10*(4), 288-304.

Kent, R. (1999). *Marketing research: Measurement, method and application*. London: International Thomson Business Press.

Leng, L. A. (2016). Facebook opens Malaysian office. *The Star Online*. Retrieved from: http://www.thestar.com.my/tech/tech-news/2016/05/05/facebook-officially-opens-malaysia-office/.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication*, *14*, 79-100.

Lewis, K. (n/d). How social media networks facilitate identity theft and fraud. *Octane Magazine*. Retrieved from: https://www.eonetwork.org/octane-magazine/special-features/social-media-networks-facilitate-identity-theft-fraud.

LexisNexis (2007). Recent case leads to confusion over 'personal information' definition. *LexisNexis*. Retrieved from: http://www.lexisnexis.com.oxfordbrookes.idm.oclc.org/uk/legal/results/enhdocview.do?docLinkInd=true&ersKey=23_T25772246707&format=GNBFULL&startDocNo=0&resultsUrlKey=0_T25772246716&backKey=20_T25772246717&csi=280746&docNo=1.

Li, K., Wang, X., Li, K., and Che, J. (2016). Information privacy disclosure on social network sites: An empirical investigation from social exchange perspective. *Business Review International*, *7*(3), 282-300.

Malaysia Government (2010). *Personal Data Protection Act*. Putrajaya: Laws of Malaysia Series.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15* (4), 336-355.

Malhotra, N. K., & Birks, D. F. (2006). *Marketing research: An applied approach (2nd European Ed.)*. Essex: Pearson Education Limited.

Matzner, T. (2014). Why privacy is not enough privacy in the context of "ubiquitous computing" and "big data". *Journal of Information, Communication and Ethics in Society*, *12*(2), 93-106.

MCMC (2016). *Internet users survey 2016: Statistical brief number twenty*. Putrajaya: MCMC.

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing*, *12*(Fall), 206-215.

Noain-Sánchez, A. (2016). "Privacy by default" and active "informed consent" by layers: Essential measures to protect ICT users' privacy". *Journal of Information, Communication and Ethics in Society*, *14*(2), 124-138.
Ninomiya, K. (2016). Invasion of privacy on social media. *LinkedIn*. Retrieved from: https://www.linkedin.com/pulse/invasion-privacy-social-media-kent-ninomiya-1.
Onn, Y. (2005). Privacy in the digital environment. In N. Elkin-Koren, & M. Birnhack, M. (Eds.), *Privacy in the digital environment*. (pp. 2-167). Haifa: Haifa Centre of Law and Technology.
Opgenhaffen, M., & Claeys, A. S. (2017). Between hope and fear: Developing social media guidelines. *Employee Relations*, *39*(2), 130-144.
Opsahl, K. (2010). Facebook's eroding privacy policy: A timeline. *Electronic Frontier Foundation*. Retrieved from: https://www.eff.org/deeplinks/2010/04/facebook-timeline.
Ozer, N. A. (2012). Putting online privacy above the fold: Building a social movement and creating corporate change. *NYU Review of Law and Social Change*, *36*, 215-28.
Pedley, P. (2002) Data protection issues for intranets and web sites. *Business Information Review*, *19*(3), 41-49.
Phelps, J., Nowak. G., & Farrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27-41.
Pierson, J., & Heyman, R. (2011). Social media and cookies: Challenges for online privacy. *Info*, *13*(6), 30-42.
Prosser, W.L. (1960). Privacy. *California Law Review*, Vol.*48*(3), 383-423.
Rainie, L., & Duggan, M. (2016). *Privacy and information sharing*. Pew Research Centre. Retrieved from: http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.
Science and Technology Committee (2014). *Responsible use of data (Fourth report of session 2014-15) – Report, together with formal minutes*. London: House of Commons, TSO (The Stationary Office).
Sherchan, W., Nepal, S., & Paris, C. (2013). A survey of trust in social networks. *ACM Computing Surveys, 45*(4), 1-33.
Statista. (2016). Daily time spent on social networking by internet users worldwide from 2012 to 2016 (in minutes). *Statista*. Retrieved from: https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/.
Steeves, V., & Regan, P. (2014). Young people online and the social value of privacy. *Journal of Information, Communication and Ethics in Society*, *12*(4), 298-313.
Suzuki, S., & Takemura, K. (2013). Culture and social media: Exploration of differences between the United States and Japan. In M. R. Olivas-Luján, & T. Bondarouk (Eds.), *Social Media in Strategic Management* (pp. 245-258). Bingley: Emerald Group Publishing Ltd.
Tan, X., Qin, L., Kim, Y., & Hsu, J. (2012). Impact of privacy concern in social networking web sites. *Internet Research*, *22*(2), 1066-2243.
Taylor, M., Haggerty, J., Gresty, D., Pacheco, N.C., Berry, T., & Almond, P. (2015). Investigating employee harassment via social media. *Journal of Systems and Information Technology*, *17*(4), 322-335.

Teensafe (2016). Cyber bullying facts and statistics. *Teensafe*. Retrieved from: https://www.teensafe.com/blog/cyber-bullying-facts-and-statistics/.
Trottier, D. (2014). Police and user-led investigations on social media. *Journal of Law, Information and Science*, *23*(1), 75–96.
UK Government (1998). *Data Protection Act*. London: Stationary Office.
Van Lieshout, M., Kool, L., Van Schoonhoven, B., & De Jonge, M. (2011). Privacy by design: An alternative to existing practice in safeguarding privacy. *Info*, *13*(6), 55-68.
Venezia, S. J. (2012). The interaction of social media and the law and how to survive the social media revolution. *New Hampshire Bar Journal*, *52*, 24-30.
Wainwright v Home Office, UKHL 53 (House of Lords October 16, 2003).
Waters, D. (1998). *Quantitative methods for business (2nd Ed.)*. Harlow: Addison Wesley Longman Publishers, Ltd.
Weller, K. (2016). Trying to understand social media users and usage: The forgotten features of social media platforms. *Online Information Review*, *40*(2), 256-264.
Whitcroft, O. (2013). Social media – challenges in the control of information. *Privacy & Data Protection, 13*(7), 7-11.
White, J. (2016). Social media user statistics in the UK. *Thelasthurdle*. Retrieved from: https://www.thelasthurdle.co.uk/social-media-user-statistics-in-the-uk-for-2015/.
Williams, R. (2016). Facebook faces ICO investigation over secret user experiment. *The Telegraph*. Retrieved from: http://www.telegraph.co.uk/technology/facebook/10940388/Facebook-faces-ICO-investigation-over-secret-user-experiment.html.
Workplace Fairness. (2017). Social networking and computer privacy. *Workplace Fairness*, Retrieved from: http://www.workplacefairness.org/social-network-computer-privacy-workplace#1.
Yong, P. K. (2009). Privacy and personal data protection in the Malaysian communications sector – Existing in a void? *MLJA*, *5*, 103.
Yusoff, Z. M. (2014). Protection of privacy in Malaysia: A law for the future. (Doctoral dissertation). Retrieved from: http://researcharchive.vuw.ac.nz/xmlui/bitstream/handle/10063/3393/thesis.pdf?sequence=2.

Jason J Turner has published, edited and reviewed articles for national and International journals for over 17 years. His research areas are principally enterprise education and the application of technology to business. He holds a number of external appointments with commercial and academic institutions and is currently the Head of Department, Postgraduate Business at Taylor's University.

Puteri Sofia Amirnuddin is a law lecturer and Programme Director for the Master of Laws programme at Taylor's University. Over a period of six years both in academia and practice, she has amassed knowledge in the areas of land and competition law. She is currently investigating the latter through a PhD programme of study. She has an emerging publication record and is actively advocating 'Augmented Reality Learning' to her students and the community.