Post Publication Review

Scott, K, Richards, D, Adhikari, R. (2015) A Review and Comparative Analysis of Security Risks and Safety Measures of Mobile Health Apps. *Australasian Journal of Information Systems*, 19, doi:http://dx.doi.org/10.3127/ajis.v19i0.1210.

Review

The above paper by Scott et al 2015, is a timely contribution to the growing literature on mobile health apps. The authors stated their aim to be "to investigate the data security and privacy features of 20 popular free and paid health apps." Furthermore, as the title of their paper makes clear, consumer safety was also an important consideration in their study, which is further borne out in their methodology. Thus their contribution draws attention to flaws in current health app designs and in international legislation and policies, which permit client data to be shared with third parties or to be stored insecurely. The background to the study, and the issues addressed in the discussion of their findings are applicable to a wide and international audience. Overall I found it to be a thorough and engaging read.

There are four areas that I wish to explore further, if the authors will respond to this review: (1) I found it curious that more was not made of the Australian context, given that the authors are in Australia and the journal targeted was Australasian. Instead the legal discussion mostly focuses on the USA, with a little also from Europe. (2) Whilst the security discussion was very thorough, and considered many viewpoints, it assumed all users are the same, when instead some are more vulnerable than others. (3) It appears to equate privacy with security. (4) Client safety is seen as very important and, following on from (2), this is particularly the case for vulnerable clients.

Firstly, on page 2 the Scott et al describe the difficulty for a client to keep abreast of legislative changes. This is indeed the case, as was recently shown not for clients, but health care providers in rural Australia (Burmeister, Islam, Dayhew, & Crichton, 2015); one example therein was that of 104 changes to the NSW State privacy legislation in a single year – clearly beyond the scope of all but legal experts to keep abreast of. However, the last paragraph of section 2.4 is very USA centric and implies that the same is true elsewhere, when at least in Australia that is not the case. For apps that store data in Australian jurisdictions, there are clear laws that govern what can be shared with third parties, about encryption and more; seen particularly in changes to the Commonwealth Privacy Act that were brought into play in mid-2014 and as a result of which there are now far greater requirements for transparency in the handling of personal information.

Secondly, all clients appear to be treated equally in this article. That in itself is curious, given that two of the apps reviewed were NeuroMind and StressCheck, apps which would be used by vulnerable consumers, many of whom could have cognitive challenges. People who are vulnerable, such as those with reduced cognitive capacity are not considered, as is evident at least by implication, by passages such as at the end of section 2.1, where it is assumed that rational choices are made by all mobile health app users. Similarly Table 3 assumes that all consumers who use the apps are rational and able to reason their way through the (sometimes bewildering) legal jargon and disclaimers. For instance, my work is mostly in areas of technology use of consumers of mental health services, where we have shown that such consumers, particularly older people, can be considered vulnerable users, whose vulnerability increases with increasing age (Bernoth, Dietsch, Burmeister, & Schwartz, 2014), and that their technology interaction needs can be different from those of younger age groups (Burmeister, 2010). Furthermore, as recently seen in this journal, people with suicidal ideation also need to be considered as not always making rational choices (Carlson, Farrelly, Frazer, & Borthwick, 2015).

The third is evident in many places. For instance, none of the measures in Table 1 are related to non-security privacy. Whereas technical matters (eg encryption) are defined, privacy is not.

At times it is used in relation to confidentiality, at other times in relation to information privacy (Cockcroft, 2006), and other uses. In fact such are all different types of privacy. The authors are not alone in failing to distinguish privacy. Almost two decades ago I pointed out that the Australian Computer Society had dropped 'confidentiality' from its code of ethics in the apparent mistaken assumption that it was the same as privacy (Burmeister, 2000) and was involved in revising that misunderstanding (Bowern, Burmeister, Gotterbarn, & Weckert, 2006).

Finally, I'd have liked to see more in-depth discussion on consumer safety, which is even more critical for vulnerable consumers: the young, people with intellectual disabilities, and older people with neuro-degenerative diseases, as shown in many recent studies (Pakrasi, Burmeister, McCallum, Coppola, & Loeb, 2015; van Wynsberghe, 2015). For instance, in discussing apps and other assistive devices for people with dementia Teipel et al. (2016) claimed that the solution involves the balance of a complex negotiation of many factors (cultural, environmental and personal factors, social resources, and advancements in the intelligence and flexibility of the technological devices), that at its center has the safety of patients.

Oliver Burmeister
Charles Sturt University
oburmeister@csu.edu.au

Author Response

We thank the reviewer for his comments on our paper, which have expanded our research findings into the security risks and safety measures of health apps and provided additional areas of future research. Our study was aimed at general populations using health apps and we acknowledge the reviewer's assertion that not all users are the same in their ability to follow the security and safety recommendations for app users. Indeed, following such recommendations may be challenging for many classes of users due to a range of factors, including time, motivation, ability (cognitive, physical, psychological) and access to resources. We agree that vulnerable users, such as the elderly and those with mental health issues have specific needs and challenges in managing privacy and security concerns. We would argue that children are another vulnerable group (Benassi, 1999; Scott, Gome, Richards, & Caldwell, 2015). However, it was, and is, beyond the scope of our investigation to suggest how our general recommendations could be modified for, or implemented by, specific groups of users. In other work, the second author has grappled with issues related to social media and social networks, such as adding friends and becoming a follower, for vulnerable populations (Ruppert, Richards, Arnold, Riches, & Parmenter, 2010) and the (in)appropriate design and use of virtual characters as buddies or companions for those with psychosis, as in the work by Bickmore, Puskar, Schlenk, Pfeifer, and Sereika (2010).

Our paper should have more clearly defined privacy and security. In a general sense, we use the word 'privacy' to refer to the rights of the individual to choose to reveal or disclose information about themselves and their property (Agrawal & Srikant, 2000), both tangible and intangible (Warren & Brandeis, 1890). In the Australian health context, a range of federal, state and territory privacy regulations limit the collection, storage, access, use and disclosure of personal identifying information (NHMRC, 2004) (p. vii), and prohibit its use or disclosure without consent for purposes other than that for which it was collected, unless there is an emergency, law enforcement justification or administrative determination (NHMRC, 2004) (p. viii). We note that, in response to the increasing use of digitisation in contemporary society, The Office of Australian Information Commissioner is developing resources offering health privacy guidance for health service providers and consumers (OAIC, 2015), in line with the Privacy Act 1988 (Australian Government, 1988).

In our paper we treat 'security' as a higher-level concept covering more than just privacy, as evidenced in Table 2. Due to the sensitive nature of medical and personal data, in our paper we have discussed both privacy and security; however, we have used the word 'security'

throughout, notably in the paper title, to recognise that security is a bigger issue than just privacy.

Our study was targeted at an international rather than an Australasian audience, so the international context we provided sought to identify the lack of legislation in much of the world, notably the USA, which is a leader in software app development. The reviewer's comments and references are valuable and provide a more local context but give the impression that due to such legislation, there is less of a problem and that app developers should have clear guidelines to follow. However, our study, which involved the most frequently accessed health apps in Australia, found that most of these apps failed to follow this legislation and in many cases may not have been bound by Australian legislation, even though they were accessed and used by Australians. This highlights the complexity and global reach of the problem, as well as issues around legal boundaries. Further research in this area would clarify the issues involved and indicate possible means of addressing them.

Karen Scott
The Children's Hospital at Westmead
University of Sydney
karen.scott@health.nsw.gov.au

Deborah Richards
Macquarie University
deborah.richards@mq.edu.au

Rajindra Adhikari
Macquarie University
rajindra.adhikari@students.mq.edu.au

References

Agrawal, R., & Srikant, R. (2000). Privacy-preserving data mining. Paper presented at the ACM Sigmod Record.

Australian Government. (1988). Privacy Act 1988. Retrieved from https://www.legislation.gov.au/Series/C2004A03712

Benassi, P. (1999). TRUSTe: an online privacy seal program. *Communications of the ACM*, 42(2), 56-59.

Bernoth, M., Dietsch, E., Burmeister, O. K., & Schwartz, M. (2014). Information Management in Aged Care: Cases of Confidentiality and Elder Abuse. *Journal of Business Ethics*, 122, 453-460. doi: 10.1007/s10551-013-1770-7

Bickmore, T. W., Puskar, K., Schlenk, E. A., Pfeifer, L. M., & Sereika, S. M. (2010). Maintaining reality: Relational agents for antipsychotic medication adherence. *Interacting with Computers*, 22(4), 276-288.

Bowern, M., Burmeister, O. K., Gotterbarn, D., & Weckert, J. (2006). ICT Integrity: Bringing the ACS Code of Ethics up to date. *Australasian Journal of Information Systems*, 13(2), 168-181.

Burmeister, O. K. (2000). Applying the ACS code of ethics. *Journal of Research and Practice in Information Technology*, 32(2), 107-120.

Burmeister, O. K. (2010). Websites for seniors: Cognitive accessibility. *International Journal of Emerging Technologies and Society*, 8(2), 99-113.

Burmeister, O. K., Islam, M. Z., Dayhew, M., & Crichton, M. (2015). Enhancing client welfare through better communication of private mental health data between rural service providers. *Australasian Journal of Information Systems*, 19, 1-14. doi:http://dx.doi.org/10.3127/ajis.v19i0.1206

Carlson, B. L., Farrelly, T., Frazer, R., & Borthwick, F. (2015). Mediating Tragedy: Facebook, Aboriginal Peoples and Suicide. *Australasian Journal of Information Systems*, 19. doi:10.3127/ajis.v19i0.1174

Cockcroft, S. (2006). Information Privacy: Culture, Legislation and User Attitudes. *Australasian Journal of Information Systems*, 14(1). doi:10.3127/ajis.v14i1.7

NHMRC. (2004). *National Health and Medical Research Council: The regulation of health information privacy in Australia*. Retrieved from http://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/nh53.pdf

OAIC. (2015). *Office of the Australian Information Commissioner: Health privacy guidance*. Retrieved from https://www.oaic.gov.au/engage-with-us/consultations/health-privacy-guidance/

Pakrasi, S., Burmeister, O. K., McCallum, T. J., Coppola, J. F., & Loeb, G. (2015). Ethical telehealth design for users with dementia. *Gerontechnology*, 13(4), 383-387. doi:10.4017/gt.2015.13.4.002.00

Ruppert, S., Richards, D., Arnold, S., Riches, V., & Parmenter, T. (2010). Applying Medicine 2.0 to the I-CAN-Managing the Needs and Rights of End Users. Paper presented at the *WEBIST* (2).

Scott, K. M., Gome, G. A., Richards, D., & Caldwell, P. H. Y. (2015). How trustworthy are apps for maternal and child health? *Health and Technology*, 4(4), 329-336. doi:10.1007/s12553-015-0099-x

Teipel, S., Babiloni, C., Hoey, J., Kaye, J., Kirste, T., & Burmeister, O. K. (2016). Information and communication technology solutions for outdoor navigation in dementia. Alzheimer's & Dementia: *The Journal of the Alzheimer's Association*, 1-13. doi:10.1016/j.jalz.2015.11.003

van Wynsberghe, A. (2015). *Healthcare Robots: Ethics, Design and Implementation*: Ashgate Publishing, Ltd.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 193-220.