

-----  
18-Feb-2021

BMJ-2020-063318 entitled "Analysing Privacy Issues of Android Mobile Health and Medical Applications"

Dear Dr. Tangari,

Thank you for sending us your paper. We sent it for external peer review and discussed it at our manuscript committee meeting. We recognise its potential importance and relevance to general medical readers and would like to offer publication in the BMJ if you are willing to revise as we suggest.

We hope very much that you will be willing and able to revise your paper as explained below in the report from the manuscript meeting. We are looking forward to reading the revised version in due course.

Please remember that the author list and order were finalised upon initial submission, and reviewers and editors judged the paper in light of this information, particularly regarding any competing interests. If authors are later added to a paper this process is subverted. In that case, we reserve the right to rescind any previous decision or return the paper to the review process. Please also remember that we reserve the right to require formation of an authorship group when there are a large number of authors.

When you return your revised manuscript, please note that The BMJ requires an ORCID iD for corresponding authors of all research articles. If you do not have an ORCID iD, registration is free and takes a matter of seconds.

Dr John Fletcher  
Associate Editor  
The BMJ  
jfletcher@bmj.com

\*\*\* PLEASE NOTE: This is a two-step process. After clicking on the link, you will be directed to a webpage to confirm. \*\*\*

[https://mc.manuscriptcentral.com/bmj?URL\\_MASK=3114cff9f05a448aa56b2876ba4d02ae](https://mc.manuscriptcentral.com/bmj?URL_MASK=3114cff9f05a448aa56b2876ba4d02ae)

\*\*Report from The BMJ's manuscript committee meeting\*\*

These comments are an attempt to summarise the discussions at the manuscript meeting. They are not an exact transcript.

Members of the committee were: Elizabeth Loder (chair); Tim Cole (statistician); Wim Weber; John Fletcher; Joseph Ross; Tiago Villanueva; Nazrul Islam

Decision: Put points

Detailed comments from the meeting:

1. The problems of data privacy in medical applications are of course important and your analysis gives us all something to think about and discuss. The paper is an unusual one for a clinical journal like the BMJ and many of the technical aspects will be beyond our readers. We will commission an accompanying editorial to go with your research and we also ask you to explain some of the technical terms where necessary. Perhaps you could ask a clinician who knows nothing of the subject to read and give feedback during the revision process.
2. Please make a clear distinction between legal and illegal data breaches. At the moment it is very difficult to get a feel for how "wrong" some of the detected behaviours are.
3. In the introduction please provide a little context for similarities and difference between Australia and, say, Europe and the USA. Are the same apps available? Are the regulatory frameworks and privacy laws comparable?
4. Please at least comment on likely similarities or differences with apps for the Apple OS.
5. Please be aware of how results may be interpreted by people less familiar with the subtleties of the inner workings of apps. For example, potentially alarming charts or statements may deter patients from enrolling in COVID-19 contact tracing apps, which may be detrimental to their own and population health. It is also possible that conspiracy theorist may misuse some results to attract people to their cause.
6. Our statistician offered the following observations
  - The cumulative distributions in Figures 2 and 7 (Please define ECDF) would be better as density distributions. -- The barcharts would be better with the total bars omitted.
  - Please present percentages as whole numbers. Decimal places add nothing useful.
7. Our patient editor asked for the following:

The authors need to add in their PPI declaration in their own words and if there was no PPI please have them share why so the statement is meaningful e.g. No funding, COVID restrictions, limited data access etc. The paper is also missing dissemination statements, this can be a good opportunity to involve one of the patient reviewers or someone in the community to co-author an Opinion piece about your research for The BMJ. The Link may be helpful  
<https://drive.google.com/file/d/14vnXwTJ2CDn2KQsuNpuEnSwad69gc7dR/view> This is a topic of great interest to the public and many have found the privacy limitations to be harmful or intrusive.

Dissemination

Please confirm when and how results were (or will be) disseminated. Guidance for best practice in dissemination is set out in the following link and gives examples:  
<https://www.nih.ac.uk/funding-and-support/documents/funding-for-research-studies/manage-my-study/How-to-disseminate-your-research/dissemination-guidance.pdf>
8. Please revise your paper to respond to all of the comments by the reviewers. Their reports are available at the end of this letter, below.

In your response please provide, point by point, your replies to the comments made by the reviewers and the editors, explaining how you have dealt with them in the paper.

#### Comments from Reviewers

Reviewer: 1

Recommendation:

Comments:

This paper may be rather esoteric for all but a small number of BMJ readers but that is not a reason to reject it. A lot of the tables and graphs should be in an appendix to reduce the complexity for the non-technical reader trying to follow the arguments. They need to be there but only for people who wish to look at the background information. Putting them online and not in the paper publication is obviously an option.

It uses techniques that I have not seen before for analysis of a medical application. Mobile health care applications are becoming important and their potential impact is unknown. This paper uses ways of analysing the software and produces an interesting output that deserves to be more widely known. There has been significant disquiet about data collection from mobile apps and what it could be used for. This paper makes a contribution to defining the scope of the problem in health care applications.

The objectives, design, interventions, and outcomes are reasonable and have been fulfilled. The results and conclusions, with minor changes, are acceptable and in my opinion an important addition to this area and may be considered ground breaking.

In conclusion I feel that this should be published with some corrections as outlined.

Dr Trefor Roscoe FFCI

#### Individual Points

Page No. 2 Line 14 (e.g., the..... Unnecessary comma should this be (For example, the .....

Page No. 4 Line 52 while paid and geoblocked apps were excluded. Can understand why but may this have introduced an unknown bias? Either the free apps captured more data to fund them, or the paid for apps were more complex had better security and were not selling data as they did not need to sell data to make it commercially viable. Difficult to unravel and would require significant funding. However, they analysed 75% of the 20,000 more than sufficient. Overall, I feel that this is not a major issue in the context of the issues revealed in this paper.

Page 12 Line 53 Insecure transmission of user data: I think most of this paragraph may be unnecessary as this is a well known problem. Could be reduced to a single sentence, "Analysing the communication leaking personal data, we observe that as much as 23% of leaks are in unencrypted HTTP traffic a known security problem."

Page 13 Line 10 et sequae. 3.4 User Perceptions of mHealth Apps This analysis is in my opinion interesting but not valid. User feedback is very variable and does not reflect the full picture. There is a bias in the data, negative feedback is much more common than positive. I do not think this can be included other than a simple statement that analysis of this area was tried but the results could not be validated. A variation on the final paragraph should suffice I would suggest "Analysis of user reviews was undertaken but because of the bias introduced by negative feedback being far more common than positive feedback, we conclude that while mHealth app users have a limited interest in (or awareness of) the apps' privacy conduct and the presence of ads/trackers and the inclusion of user data collection operations the significance is not clear."

#### Additional Questions:

**The BMJ** uses compulsory open peer review. Your name and institution will be included with your comments when they are sent to the authors. If the manuscript is accepted, your review, name and institution will be published alongside the article.

If this manuscript is rejected from **The BMJ**, it may be transferred to another BMJ journal along with your reviewer comments. If the article is selected for publication in another BMJ journal, depending on the editorial policy of the journal your review may also be published. You will be contacted for your permission before this happens.

For more information, please see our [peer review terms and conditions](https://www.bmj.com/about-bmj/resources-reviewers).

**Please confirm that you understand and consent to the above terms and conditions.**  
I consent to the publication of this review

Please enter your name: Dr Trefor Roscoe FFCI

Job Title: Medical Information Consultant

Institution: None

Reimbursement for attending a symposium?: No

A fee for speaking?: No

A fee for organising education?: No

Funds for research?: No

Funds for a member of staff?: No

Fees for consulting?: No

Have you in the past five years been employed by an organisation that may in any way gain or lose financially from the publication of this paper?: No

Do you hold any stocks or shares in an organisation that may in any way gain or lose financially from the publication of this paper?: No

If you have any competing interests <a href="http://www.bmj.com/about-bmj/resources-authors/forms-policies-and-checklists/declaration-competing-interests" target="\_new"> (please see BMJ policy) </a> please declare them here: None

<em>BMJ are working with <a href="https://orcid.org/" target="\_blank">ORCID</a> to recognise the importance of the reviewer community. Reviewers are now able to share their activity by connecting their review to their ORCID account to gain recognition for their contributions.</em>

Only the Journal title will be uploaded into the reviewer's ORCID record, along with the date the record was uploaded; there is no identification of the article's title or authors. Records are uploaded once a decision (accept, reject, or revision) has been made on the article.</em>

Would you like to be accredited by <a href="https://orcid.org/" target="\_blank">ORCID</a> for this review?: No

Reviewer: 2

Recommendation:

Comments:

The study presented the data collection practices and analysed the current state of mHealth apps on google play. As indicated in the paper, Google requires the app developers to disclose the collection and sharing of user data. It will be informative to present the correlation between third party presence in app resources, access to personal data in the app code and privacy policy.

As indicated by the authors, the analysis is based on automated testing platform, not involving users or developers. Thus, providing user perceptions of mHealth Apps based on negative reviews only would not represent the user perception. Having said that, the study can be indicated as the results of automated testing and evaluation but to draw the conclusion of user awareness. Privacy and confidentiality concerns are for any online forum or applications and comparison of mHealth apps and other apps would be informative. It is noted that the apps have been categorised as medical and health and fitness in the manuscript. Could you please clarify the definitions used to categorise medical apps in the manuscript. Are these the medical devices that identified by FDA or TGAs? Privacy and data collection of these would be of interest to clinicians and patients and that would be an important contribution to the literature and also reflecting of the privacy requirements from NHMRC guidelines or the Privacy guideline in Australia or the specific health privacy requirements from the jurisdiction. There would be some health and fitness app that access personal information and monitor their health progress with the consumer's consent and share information to the third party with their consent. Thus, the purpose of the apps and the privacy policy needs to be considered. The study concluded that the mHealth apps are far from transparent when dealing with user data. However, it has not been presented in the article the correlation between them. Several fitness apps and several other apps are under the category of health and wellness application in the google play store but they are not the decision support tools for clinicians as indicated in the article section 5, line 40. The paper could be expanded to discuss comprehensively on privacy issues or presented as the comparison of data collections providing the open question.

**Additional Questions:**

**The BMJ** uses compulsory open peer review. Your name and institution will be included with your comments when they are sent to the authors. If the manuscript is accepted, your review, name and institution will be published alongside the article.

If this manuscript is rejected from **The BMJ**, it may be transferred to another BMJ journal along with your reviewer comments. If the article is selected for publication in another BMJ journal, depending on the editorial policy of the journal your review may also be published. You will be contacted for your permission before this happens.

For more information, please see our [peer review terms and conditions](https://www.bmj.com/about-bmj/resources-reviewers).

**Please confirm that you understand and consent to the above terms and conditions:**  
I consent to the publication of this review

Please enter your name: Khin Than Win

Job Title: Associate Professor

Institution: University of Wollongong

Reimbursement for attending a symposium?: No

A fee for speaking?: No

A fee for organising education?: No

Funds for research?: No

Funds for a member of staff?: No

Fees for consulting?: No

Have you in the past five years been employed by an organisation that may in any way gain or lose financially from the publication of this paper?: No

Do you hold any stocks or shares in an organisation that may in any way gain or lose financially from the publication of this paper?: No

If you have any competing interests <a href="http://www.bmj.com/about-bmj/resources-authors/forms-policies-and-checklists/declaration-competing-interests" target="\_new"> (please see BMJ policy) </a> please declare them here: None.

<em>BMJ are working with <a href="https://orcid.org/" target="\_blank">ORCID</a> to recognise the importance of the reviewer community. Reviewers are now able to share their activity by connecting their review to their ORCID account to gain recognition for their contributions.</em>

Only the Journal title will be uploaded into the reviewer's ORCID record, along with the date the record was uploaded; there is no identification of the article's title or authors. Records are uploaded once a decision (accept, reject, or revision) has been made on the article.</em>

Would you like to be accredited by <a href="https://orcid.org/" target="\_blank">ORCID</a> for this review?: Yes

Reviewer: 3

Recommendation:

Comments:

This is article has a lot of relevance in the current environment, firstly due to increased isolation caused by the COVID pandemic and secondly due to the increased use of mobile health and fitness apps by the general public, patients and by clinicians.

1. Fix grammatical errors in the text. Last paragraph in section 1 Introduction, Insert a "to" after order.
2. Table 1. Consider add "Yes" and " No" above columns in rows "Contains Ads..." and " Includes privacy link ...."
3. Table 1. There is a duplicate "privacy" word in the row "includes privacy link..."
4. Define ECDF in Figure. 2
5. In Figure 4 define All. Is this all mHealth apps?

6. In Figure 5 consider first 10 sets of libraries as for others the results are negligible. If its important to list all, the results for the remainder can be added in an appendix.

7. In Figure 6 it is difficult to differentiate the difference between various add and tracker domains. Suggest only listing the major ones.

8. In Table 5 it seems that no privacy policy column defines where privacy policy exists but does not cover certain data leaks. Reword this column. However if there is no privacy policy , how can we say there is compliance or violation regarding data leaks?

9. Table 6. What is the basis of the PP violation %.

10. It is great that the authors have highlighted a problem, however, it would be useful to incorporate a comprehensive section of what steps patients and clinicians can carry out to ensure that they use apps that are compliant with national data privacy guidelines such as GDPR. In addition what action can Google take to reduce lack of privacy policy implementations and to increase compliance with stored privacy policies and to national guidelines?

Additional Questions:

***The BMJ*** uses compulsory open peer review. Your name and institution will be included with your comments when they are sent to the authors. If the manuscript is accepted, your review, name and institution will be published alongside the article.

If this manuscript is rejected from *The BMJ*, it may be transferred to another BMJ journal along with your reviewer comments. If the article is selected for publication in another BMJ journal, depending on the editorial policy of the journal your review may also be published. You will be contacted for your permission before this happens.

For more information, please see our [peer review terms and conditions](https://www.bmj.com/about-bmj/resources-reviewers).

**Please confirm that you understand and consent to the above terms and conditions.**  
I consent to the publication of this review

Please enter your name: Dr Manzoor Ahmed

Job Title: CEO

Institution: HIGOE Ltd

Reimbursement for attending a symposium?: No

A fee for speaking?: No

A fee for organising education?: No

Funds for research?: No

Funds for a member of staff?: No

Fees for consulting?: No

Have you in the past five years been employed by an organisation that may in any way gain or lose financially from the publication of this paper?: No

Do you hold any stocks or shares in an organisation that may in any way gain or lose financially from the publication of this paper?: No

If you have any competing interests <a href="http://www.bmj.com/about-bmj/resources-authors/forms-policies-and-checklists/declaration-competing-interests" target="\_new"> (please see BMJ policy) </a> please declare them here:

<em>BMJ are working with <a href="https://orcid.org/" target="\_blank">ORCID</a> to recognise the importance of the reviewer community. Reviewers are now able to share their activity by connecting their review to their ORCID account to gain recognition for their contributions.</em>

Only the Journal title will be uploaded into the reviewer's ORCID record, along with the date the record was uploaded; there is no identification of the article's title or authors. Records are uploaded once a decision (accept, reject, or revision) has been made on the article.</em>

Would you like to be accredited by <a href="https://orcid.org/" target="\_blank">ORCID</a> for this review?: Yes

Reviewer: 4

Recommendation:

Comments:

I enjoyed reading this important paper that analyzed the privacy issues of Android mobile health applications. This study is expansive in scope, and employed rigorous methods to elucidate interesting insights.

Here are my thoughts and suggestions for consideration:

1) Consider articulating how the android apps are positioned within the larger 'market' that consists of apps from other platforms (e.g., Apple). In particular, what is the market capture of android health/wellness apps as compared to Apple? Do Android health/wellness apps make up just 10% or perhaps 60%? Presenting the 'market' context will help articulate the representativeness of the data.

2) Consider stating explicitly the paper's conceptual significance. From my reading, the key contribution is providing a framework to analyze privacy of mobile apps. Consider expounding on this.

3) The authors made a good point that theirs is one of the first studies to analyze privacy metrics in Android mobile health apps. In the introduction, consider stating how serious is the privacy issue? This adds to the conceptual significance of the paper.



4) The practical significance could also be discussed. For example, what do the findings mean for policy? What are the implications for data security and protection? How could Google use these findings to improve their privacy policies? How do clinicians better articulate the benefits/risk of apps to patients based on the findings of this important study?

5) The paper excels in detail and rigor, however I found that the key topic of privacy is somewhat distracted by the many sub-topics and figures. Consider a sharper focus in the main text and its figures, and relegating the other impressive, albeit tangential, figures to the supplementary document.

6) A small typo in the Abstract ("objective"): "To investigate whether and what user data is..." It should be "data are" as the singular form is datum.

**Additional Questions:**

**The BMJ** uses compulsory open peer review. Your name and institution will be included with your comments when they are sent to the authors. If the manuscript is accepted, your review, name and institution will be published alongside the article.

If this manuscript is rejected from **The BMJ**, it may be transferred to another BMJ journal along with your reviewer comments. If the article is selected for publication in another BMJ journal, depending on the editorial policy of the journal your review may also be published. You will be contacted for your permission before this happens.

For more information, please see our [peer review terms and conditions](https://www.bmj.com/about-bmj/resources-reviewers).

**Please confirm that you understand and consent to the above terms and conditions:**  
I consent to the publication of this review

Please enter your name: Reuben Ng

Job Title: Faculty

Institution: Lee Kuan Yew School of Public Policy, National University of Singapore

Reimbursement for attending a symposium?: No

A fee for speaking?: No

A fee for organising education?: No

Funds for research?: No

Funds for a member of staff?: No

Fees for consulting?: No

Have you in the past five years been employed by an organisation that may in any way gain or lose financially from the publication of this paper?: No

Do you hold any stocks or shares in an organisation that may in any way gain or lose financially from the publication of this paper?: No

If you have any competing interests <a href="http://www.bmj.com/about-bmj/resources-authors/forms-policies-and-checklists/declaration-competing-interests" target="\_new"> (please see BMJ policy) </a> please declare them here:

<em>BMJ are working with <a href="https://orcid.org/" target="\_blank">ORCID</a> to recognise the importance of the reviewer community. Reviewers are now able to share their activity by connecting their review to their ORCID account to gain recognition for their contributions.

Only the Journal title will be uploaded into the reviewer's ORCID record, along with the date the record was uploaded; there is no identification of the article's title or authors. Records are uploaded once a decision (accept, reject, or revision) has been made on the article.</em>

Would you like to be accredited by <a href="https://orcid.org/" target="\_blank">ORCID</a> for this review?: Yes

Reviewer: 5

Recommendation:

Comments:

Thank you for the opportunity to review this manuscript. The authors conducted a large-scale analysis of the privacy and data sharing practices of a sample of more than 20,000 medical, health and fitness apps available in the Australian Google Play store for the Android platform. While other analyses of data sharing practices have been conducted at scale, this analysis focuses on health apps.

The authors confirm previous analyses of health apps in finding that the majority of sampled apps collect and share user information with third-parties that provide analytics and advertising services. They further analyse data sharing practices against stated privacy policies, confirming a large literature that suggest that privacy policies are lacking detail and transparency. The most novel aspect of the study was to analyse public app reviews through a privacy lens using machine learning methods, noting that user complaints and awareness of privacy risks are rare.

Please note that I am not qualified to critique the machine learning or other code/traffic analysis methods in detail, but did note that further information on the sensitivity/specificity of the approach may be useful in a supplementary file.

Overall, the authors have conducted a large-scale and comprehensive analysis of mobile health apps in the Australian Google Play store, triangulating data from multiple unique analyses. The paper could be strengthened by highlighting the key gaps in the literature – much of what the authors do replicates and confirms smaller-scale analyses – and emphasising what the 'scale' adds. The paper is long for a clinician audience in its current form and so really emphasising what these analyses add, what is novel and ensuring that all analyses are well-integrated and justified would make this more impactful.

Major comments:

I would suggest that the introduction focus squarely on the state of mHealth in relation to privacy. For example, while the authors discuss issues related to efficacy and clinical safety, greater focus could be had from explicating what is known about mHealth data privacy. Further, developments like the FDA guidance should be described in terms of how they address privacy. The summary of key findings may be better placed in the first paragraph of the Discussion; the Introduction should instead explicitly state the gaps that this paper will fill given that there have been numerous recent analyses of data sharing practices of mHealth apps.

Specifically, what does a large-scale analysis add to our understanding of risks and benefits of mHealth? Much of what is currently located in the 'Comparison to other studies section' could be beneficial in the introduction to highlight what this study adds.

The authors present information in Figure 3 contrasting the practices between health apps and non health apps. This strikes me as particularly novel and a key contribution to the literature, but it is given little attention in the introduction/study aims and could be made more of in the results/discussion. This also strikes me as the key contribution of a large-scale analysis.

A strength of this analysis is that the authors employ three distinct methods of analysing privacy/data sharing practices: static file/code analysis, dynamic traffic analysis, and privacy policy analysis. However, greater clarity around their respective strengths/limitations and integration of these findings is required.

First, the authors variably use the terms "data collection practice," "leaks" and "operations involving personal data." This needs to be clarified right up front and consistent terminology used. It is particularly unclear what constitutes a 'leak' (ie does this apply to data sharing intended by the developer?) This is particularly important for the analysis of privacy policies as it is unclear exactly what the authors measured in terms of comparing "data leaks" to privacy policies. Thus, I was unsure what exactly constituted a "violation." Further, I did not understand how the proportion of violations was calculated – what constitutes a 'single' privacy leak for example? What is the denominator?

The authors do not distinguish between actual and potential data sharing, which I think may be a more accurate representation of what is measured. Previous analyses of apps found that static code analysis can detect possible or potential data sharing, but that often embedded ad libraries, for example, often go unused. The dynamic traffic analysis is a point in time analysis of actual data sharing. The authors should consider how these measurements can be compared and contrasted to provide a more nuanced picture, but I think it is inappropriate to simply combine these findings as "data collection practices."

Similarly, in characterizing sharing with third-parties, the findings of third-party sharing in the static file code should be separated from those in the dynamic traffic analysis in terms of possible vs actual (or as the authors state, integrated vs interacting). For example, the proportion sharing with third parties is much lower in the dynamic traffic analysis.

It is not surprising that among Android apps, the vast majority have Google services embedded in their code – could this be an artefact of Google's developer services? Further, without analysis of iOS apps, the role of Google within the greater mobile ecosystem should not be overstated. I wonder if the analysis would be more meaningful with Google's services removed? Or to do a sensitivity type analysis of third party entities without Google's services?

On page 10, line 45-48, the authors analyse the types of user data against the categories of third-party entities; this seems especially interesting and important for understanding the nature and level of privacy risk. This could perhaps be highlighted or further analysed. For example, in Table 3, could the types of data be analysed against categories of third-party? Most of these company names will not be recognizable by the average clinician reader.

In describing the integration of third-party libraries, I think the authors are referring to ad libraries, but this should be described very explicitly for a generalist, clinician audience (ie what they are and how they work). The findings in Table 2 underscore why the static code analysis and traffic analysis results

should be treated separately and triangulated rather than combined – there are discrepancies between what trackers exist in the code and which are deployed.

The description and rationale for the analysis of HTTPS transmission of user data was missing from the introduction and methods. To better integrate with the other analyses, the authors should first explain the significance of HTTPS in relation to the privacy practices analyses.

In analysing the privacy-related user complaints, more detail on what was considered 'privacy-related' would be useful for the reader. For example, the presence of ads may be "annoying" to app users (without explicitly identifying a privacy problem) and yet, still pose a privacy problem. Would these be considered privacy-related complaints? Further, in Australia, where there is a Privacy Commissioner and privacy principles, apps users may have other recourses for privacy complaints and compliant privacy policies should identify the contact information for the person responsible for handling complaints. Was this detected in the privacy policy analysis? App reviews may thus not be representative in terms of the destination for privacy-related concerns, so I would suggest taking care with interpretations/conclusions that app users are "uninterested" or "unaware", but would instead stress the correlation between privacy practices and review content.

Minor comments:

The abstract could be edited for clarity (e.g. "detected data-collection practices are towards the app developers. . .")

In the abstract, please quantify "a small number of third-parties" received 67.8% of the collected data.

The abstract results refers to data collection and also data leaks – could you define and differentiate these two instances?

The paper could be edited to reduce the word count quite significantly. The authors helpfully provide several 'road map' type statements throughout to direct the reader, but this might be more succinctly replaced with strategic headings and sub headings.

The scale of Figure 5 made it very difficult to read.

Figure 7 – what is ECDF? This should be spelled out in the legend. I did not understand what units were measured on each of the axes in Figure 7.

In the Discussion, you might need to define IMEI and MAC address for a generalist audience – what are these and what is their significance? (or perhaps simply refer to "persistent identifiers" and explain elsewhere in the paper why this is a category of data of concern).

It may be of interest to readers to have some information about the sensitivity/specificity of machine learning methods available in a supplementary files. You mention 96% accuracy in the Discussion, but this is the first mention of this in the paper.

The conclusion in part, emphasises the security of data transmission, which seemed a minor part of the analysis. This should either be included as a key aim and justified as a key analysis, or minimised in the conclusion.

Additional Questions:

**The BMJ** uses compulsory open peer review. Your name and institution will be included with your comments when they are sent to the authors. If the manuscript is accepted, your review, name and institution will be published alongside the article.

If this manuscript is rejected from *The BMJ*, it may be transferred to another BMJ journal along with your reviewer comments. If the article is selected for publication in another BMJ journal, depending on the editorial policy of the journal your review may also be published. You will be contacted for your permission before this happens.

For more information, please see our [peer review terms and conditions](https://www.bmj.com/about-bmj/resources-reviewers).

**Please confirm that you understand and consent to the above terms and conditions.**  
I consent to the publication of this review

Please enter your name: Quinn Grundy

Job Title: Assistant Professor

Institution: University of Toronto

Reimbursement for attending a symposium?: No

A fee for speaking?: No

A fee for organising education?: No

Funds for research?: No

Funds for a member of staff?: No

Fees for consulting?: No

Have you in the past five years been employed by an organisation that may in any way gain or lose financially from the publication of this paper?: No

Do you hold any stocks or shares in an organisation that may in any way gain or lose financially from the publication of this paper?: No

If you have any competing interests [please declare them here](http://www.bmj.com/about-bmj/resources-authors/forms-policies-and-checklists/declaration-competing-interests): (please see BMJ policy)

*BMJ* are working with [ORCID](https://orcid.org/) to recognise the importance of the reviewer community. Reviewers are now able to share their activity by connecting their review to their ORCID account to gain recognition for their contributions.

Only the Journal title will be uploaded into the reviewer's ORCID record, along with the date the record was uploaded; there is no identification of the article's title or authors. Records are uploaded once a decision (accept, reject, or revision) has been made on the article.

Would you like to be accredited by [ORCID](https://orcid.org/) for this review?: Yes