Gauging the acceptance of contact tracing technology: An empirical study of Singapore residents' concerns with sharing their information and willingness to trust

Ee-Ing Ong
Singapore Management University, eeingong@smu.edu.sg

Wee Ling LOO
Singapore Management University, wlloo@smu.edu.sg

Citation

Ong, Ee-Ing and LOO, Wee Ling. Gauging the acceptance of contact tracing technology: An empirical study of Singapore residents' concerns with sharing their information and willingness to trust. (2022). *Regulatory Insights on Artificial Intelligence: Research for Policy*. 71-101.
Available at: https://ink.library.smu.edu.sg/sol_research/3282

GAUGING THE ACCEPTANCE OF CONTACT TRACING TECHNOLOGY: AN EMPIRICAL STUDY OF SINGAPORE RESIDENTS' CONCERNS AND TRUST IN INFORMATION SHARING

ONG Ee Ing & LOO Wee Ling[*]

ABSTRACT

In response to the COVID-19 pandemic, governments began implementing various forms of contact tracing technology. Singapore's implementation of its contact tracing technology, TraceTogether, however, was met with significant concern by its population, with regard to privacy and data security. This concern did not fit with the general perception that Singaporeans have a high level of trust in its government. We explore this disconnect, using responses to our survey (conducted pre-COVID-19) in which we asked participants about their level of concern with the government and business collecting certain categories of personal data. The results show that respondents had less concern with the government as compared to a business collecting most forms of personal data. Nonetheless, they still had a moderately high level of concern about sharing such data with the government. We further found that income, education and perceived self-exposure to AI are associated with higher levels of concern with the government collecting personal data relevant to contact tracing, namely health history, location and social network friends' information. This has implications for Singapore residents' trust in government collecting data and hence the success of such projects, not just for contact tracing purposes but for other government-related data collection undertakings.

KEYWORDS
AI; contact tracing; COVID-19; empirical work; survey; data privacy; data security; surveillance; trust

I. INTRODUCTION

In 2020, the COVID-19 virus swept across the world. Given its high rate of infection, many countries,[1] including the Singapore government, emphasised the need for contact tracing.[2] In

[*] Ong Ee Ing, Senior Lecturer, Singapore Management University & Loo Wee Ling, Associate Professor (Education), Singapore Management University.
The authors would like to thank Huang Tengjiao (PhD candidate, SMU School of Social Sciences) and Alicia Wee, Research Associate at the Center for AI & Data Governance (Singapore Management University) for their thorough research assistance, as well as Associate Professor Tan Hwee Hoon (Singapore Management University) & Senior Lecturer Rosie Ching (Singapore Management University) for their invaluable advice.
This research is supported by the National Research Foundation, Singapore under its Emerging Areas Research Projects (EARP) Funding Initiative. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not reflect the views of National Research Foundation, Singapore.

[1] See, e.g. "The world embraces contact-tracing technology to fight COVID-19" (Bloomberg) https://www.bloomberg.com/news/articles/2020-04-30/the-world-embraces-contact-tracing-technology-to-fight-covid-19> accessed 14 December 2020.

[2] See, e.g., "Help speed up contact tracing with TraceTogether" (*Gov.Sg*) <https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether> accessed 7 October 2020.

Singapore, the government encouraged the use of the local tracing app, TraceTogether[3] and subsequently introduced the wearable tracking device, the TraceTogether token.[4]

The main alternative to the government-initiated contact tracing technology has been the one offered by the business organisations, Apple and Google. Apple and Google's technology provided greater privacy to individuals as users at risk were alerted without their identities being released to the authorities, allowing them discretion to volunteer the information "when, for example, they register for a test".[5] However, the Singapore government had ruled out using this technology, on the basis (among other reasons) that the very advantage of Apple and Google's technology limited its capacity for effective identification of the source of infection and the chain of transmission.[6]

The government's promotion of its own TraceTogether technology, however, was not well accepted by Singapore residents. Since its launch in late March 2020, uptake of the app was low;[7] by August 2020, only 2.4 million residents had downloaded it[8] although for the technology to be effective, about 75% of Singapore's 5.7 million residents must have the app on their smartphones.[9]

It was only in late December 2020 that the adoption rate surpassed 70% when "more than two million people [had] downloaded the TraceTogether mobile application and 1.75 million tokens [had] been distributed".[10] Significantly, this was after the government's October announcement that it would be mandatory to use TraceTogether (either in app or token form) in multiple venues by December 2020, and that Phase 3, a phase that allowed more freedom of

[3] 'Singapore Launches TraceTogether Mobile App to Boost COVID-19 Contact Tracing Efforts' (*CNA*) <https://www.channelnewsasia.com/news/singapore/covid19-trace-together-mobile-app-contact-tracing-coronavirus-12560616> accessed 7 August 2020.

[4] The Singapore government is also promoting the use of the TraceTogether token, which exchanges Bluetooth signals with other tokens nearby or with mobile phones that are running the TraceTogether mobile application. "TraceTogether token to be distributed nationwide from Sept 14; new self-check, SMS alert services to be rolled out" (*Today Online*, 5 October 2020) <https://www.todayonline.com/singapore/tracetogether-token-be-distributed-nationwide-sept-14-new-self-check-sms-alert-services-be> accessed 7 October 2020.

[5] "TraceTogether: Singapore turns to wearable contact-tracing Covid tech" (*BBC* July 2020) <https://www.bbc.com/news/technology-53146360> (accessed 11 October 2020).

[6] "Two reasons why Singapore is sticking with TraceTogether's Protocol" <https://www.tech.gov.sg/media/technews/two-reasons-why-singapore-sticking-with-tracetogether-protocol> (accessed 31 October 2020). The Singapore government also noted that the Apple and Google technology could only run on later models of smartphones and not everyone in Singapore can afford one.

[7] See also "Singapore Built a Coronavirus App, but It Hasn't Worked So Far" (*WSJ*, April 2020) <https://www.wsj.com/articles/singapore-built-a-coronavirus-app-but-it-hasnt-worked-so-far-11587547805> (accessed 15 October 2020).

[8] "Low community prevalence of COVID-19, 0.03% of people with acute respiratory infection test positive: Gan Kim Yong" (*CNA*, September 2020) <https://www.channelnewsasia.com/news/singapore/covid-19-singapore-low-community-prevalence-testing-13083194> (accessed 15 October 2020).

[9] "Singapore Built a Coronavirus App, but It Hasn't Worked So Far" (*WSJ*, April 2020) <https://www.wsj.com/articles/singapore-built-a-coronavirus-app-but-it-hasnt-worked-so-far-11587547805> (accessed 15 October 2020) ("But for the technology to be effective, three-quarters of the city-state's 5.7 million residents must have the app on their smartphones, officials have said. A month after its launch, Singapore is far from that target. As of last week, TraceTogether had 1.08 million users, a government spokeswoman said").

[10] "TraceTogether adoption rate surpasses 70%, more distribution points to reopen from January 2021" (*Today*, December 2020) <https://www.todayonline.com/singapore/tracetogether-adoption-rate-surpasses-70-more-distribution-points-reopen-january-2021> (accessed 26 December 2020).

movement, would not occur until there was widespread adoption of the technology.[11] Of note, while the October announcement incentivised more to collect the tokens, reports surfaced soon after that there were individuals making unauthorised modifications to prevent the tokens from working as intended and urging others to do the same.[12]

The reluctance of some residents to use the app had been attributed to practical issues,[13] especially the way the app drained iPhone batteries.[14] However, there were also significant privacy and data security concerns surrounding the app[15] which were not ameliorated by the subsequent rollout of the token.[16] In fact, the introduction of the token triggered a public petition which warned of the danger of Singapore becoming a "surveillance state" should adoption of the token be made mandatory.[17] Indeed, despite repeated government assurances about data safety (because of the promise to confine use of data collected for contact tracing only and to restrict its period of retention) and privacy (as the app or token does not track users' location),[18] some residents still harboured concerns over these issues.[19] In this respect, an academic had opined in May 2020 that there could be a trust issue in reaction to past incidents of cyberattacks on government databases that resulted in massive data breaches.[20] As it was,

[11] "Compulsory to use TraceTogether to check in at venues such as malls, schools, workplaces by December: Govt" (*Today*, October 2020) <https://www.todayonline.com/singapore/compulsory-use-tracetogether-check-venues-such-malls-schools-workplaces-december-govt> (accessed 26 October 2020).

[12] "TraceTogether tokens allegedly modified by some" https://www.straitstimes.com/singapore/tracetogether-tokens-allegedly-modified-by-some> (accessed 31 October 2020).

[13] For example, the need to "hunt down the app" as it was released as a standalone app: see "Given low adoption rate of TraceTogether, experts suggest merging with SafeEntry or other apps" <https://www.todayonline.com/singapore/given-low-adoption-rate-tracetogether-experts-suggest-merging-safeentry-or-other-apps> (*Today*, 9 May 2020) accessed 7 October 2020; and the lack of marketing: see "Coronavirus: why aren't Singapore residents using the TraceTogether contact-tracing app?" (*SCMP*, 18 May 2020) <https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether> accessed 7 October 2020.

[14] 'Attitudes towards the Use of Surveillance Technologies in the Fight against COVID-19' <https://lkyspp.nus.edu.sg/docs/default-source/ips/ips-report-on-attitudes-towards-the-use-of-surveillance-technologies-in-the-fight-against-covid-19-240520.pdf> accessed 7 October 2020. <https://www.todayonline.com/singapore/given-low-adoption-rate-tracetogether-experts-suggest-merging-safeentry-or-other-apps> (*Today*, 9 May 2020) accessed 7 October 2020.

[15] "Coronavirus: why aren't Singapore residents using the TraceTogether contact-tracing app?" (*SCMP*) < https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether > accessed 29 December 2020.

[16] The token merely addressed the practical issues of iPhone battery-drainage and accessibility to the contact tracing scheme by people who could not afford smartphones: see "Two reasons why Singapore is sticking with TraceTogether's Protocol" <https://www.tech.gov.sg/media/technews/two-reasons-why-singapore-sticking-with-tracetogether-protocol> (accessed 31 October 2020).

[17] "Singapore says 'No' to wearable devices for Covid-19 contact tracing" (*change.org*) <https://www.change.org/p/singapore-government-singapore-says-no-to-wearable-devices-for-covid-19-contact-tracing?fbclid=IwAR23Wqo1tvznlxK9e-xOnUGz99z_ZCitqA9amEfmo5NEewt-YGvtIpiuVJU> accessed 15 December 2020. As of 16 December 2020, the petition had garnered above 54,000 signatures.

[18] See, e.g., "Help speed up contact tracing with TraceTogether" (*Gov.Sg*) <https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether> accessed 7 October 2020. See also "New TraceTogether token to have no GPS or internet connectivity to track user's whereabouts: Vivian Balakrishnan" (*Today Online*) < https://www.todayonline.com/singapore/tracetogether-token-has-no-gps-or-internet-connectivity-track-users-whereabouts-vivian> accessed 28 December 2020.

[19] "Coronavirus: why aren't Singapore residents using the TraceTogether contact-tracing app?" (*SCMP*, 18 May 2020) <https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether> accessed 7 October 2020; "Given low adoption rate of TraceTogether, experts suggest merging with SafeEntry or other apps" (*Today*, 8 May 2020) <https://www.todayonline.com/singapore/given-low-adoption-rate-tracetogether-experts-suggest-merging-safeentry-or-other-apps> (accessed 7 October 2020).

[20] See, e.g., comment by Teo Yi-Ling, a senior fellow at the S. Rajaratnam School of International Studies' Centre of Excellence for National Security, cited in "Coronavirus: why aren't Singapore residents using the

the issue of trust came to the fore when the government revealed in January 2021 that TraceTogether data could and had been accessed by the police for criminal investigations, as permitted by extant criminal procedural law.[21] Numerous residents expressed resentment at having been "betrayed" even as the government sought to explain its actions. Soon after, the government took legislative action to limit the use of TraceTogether data to investigations of serious crimes only.[22]

The patent data privacy and security concerns of some residents and their distrust in the government contact tracing technology (which was then exacerbated by the January 2021 revelation) provides an interesting counterpoint to the perception that Singapore residents generally trust the government, perhaps more so than they trust business organisations.[23] This phenomenon flags the need for further investigation as the issue of trust is important. The mere act of downloading the app or collecting the token does not mean that people will use the technology. As mentioned, some individuals who had collected the tokens were reported to have made modifications to prevent them from working.[24] After the initial download, people could also delete the app from their phones, as some had done even before the January 2021 revelation.[25] This would defeat the purpose of using the technology for contact tracing. For these reasons, we investigate the following questions in this chapter:

First, given the alternative offered by Google and Apple which has been adopted by a growing list of countries,[26] would Singapore residents have more trust in (that is, have less concern about) the use of contact tracing technology introduced by business organisations compared to government-initiated technology? To the degree that contact tracing technologies are perceived

TraceTogether contact-tracing app?" (*SCMP*, 18 May 2020) <https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether> accessed 7 October 2020. She highlighted the incident in June 2018 "when hackers copied the hospital records of more than 1.5 million patients, of which 160,000 had information about their outpatient dispensed medicines taken, in an incident described by authorities as the "most serious breach of personal data".

[21] "'Feeble' efforts by the Government to handle backlash on TraceTogether data" (*Today*, 7 January 2021) <https://www.todayonline.com/voices/feeble-efforts-government-handle-backlash-tracetogether-data?cid=emarsys-today_TODAY%27s%20morning%20briefing%20for%20Jan%208,%202021%20%28ACTIVE%29_newsletter_08012021_today> (accessed 27 February 2021).

[22] "Some TraceTogether users upset with Govt's revelation on police access to data, say they'll use it less" (*Today*, 7 January 2021) <https://www.todayonline.com/singapore/some-tracetogether-users-upset-govts-revelation-police-access-data-say-theyll-use-it-less?cid=emarsys-today_TODAY%27s%20morning%20briefing%20for%20Jan%207,%202021%20%28ACTIVE%29_newsletter_07012021_today> (accessed 27 February 2021). "Vivian Balakrishnan says he 'deeply regrets' mistake on TraceTogether data" (*StraitsTimes*, 2 February 2020) <https://www.straitstimes.com/singapore/vivian-balakrishnan-says-he-deeply-regrets-mistake-on-tracetogether-data-first-realised-it> (accessed 27 February 2021). "Bill limiting police use of TraceTogether data to serious crimes passed" (*StraitsTimes*, 2 February 2020) < https://www.straitstimes.com/singapore/politics/bill-limiting-use-of-tracetogether-for-serious-crimes-passed-with-govt-assurances> (accessed 27 February 2021).

[23] See discussion in Section II Literature Review.

[24] "TraceTogether tokens allegedly modified by some" https://www.straitstimes.com/singapore/tracetogether-tokens-allegedly-modified-by-some> (accessed 31 October 2020).

[25] For instance, in a YouGov survey conducted in December 2020, 11% of the respondents said they had downloaded the app but then deleted it: "TraceTogether adoption up to more than 60% as privacy concerns wane; users still bothered about battery drain" (*CNA*, December 2020) <https://www.channelnewsasia.com/news/singapore/tracetogether-app-token-adoption-phase-3-13748714> (accessed 26 December 2020).

[26] For the list of countries that have adopted the Apple and Google contact tracing app, see https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/ (accessed 31 October 2020).

to collect many types of users' personal data, the level of concern about sharing (or the willingness to share) such data with the data-collecting entity provides a gauge as to the level of trust reposed in the entity. A user with a high level of concern would be less willing to share his data, indicating less trust in the data-collecting entity.

Second, even if Singapore residents do, in general, repose greater trust in the government compared to businesses, what types of personal data would they still consider important to protect from the government, whether motivated by a desire to preserve privacy (and not be subject to surveillance) or ensure safety of their data from unauthorised government use or leakage to unauthorised parties? In this connection, anecdotal evidence shows that some residents perceive that the TraceTogether technology downloaded on their phone would allow the government access to other information on their phones, such as their location, health history, and contacts.[27]

Finally, what are some basic demographic characteristics that typify those who possess more data privacy or security concerns about government collection of their data, especially data that are of particular relevance to contact tracing technology?[28] Examination of relevant demographic factors could be helpful in the successful deployment of the technology. Conversely, investing without recognizing potential factors in adopters' willingness to use the technology "may lead to a waste of resources".[29]

In this respect, a survey we carried out in late 2019 provides insights into these three questions. Our survey was on the attitudes of Singapore residents towards business organisations' use of artificial intelligence ("AI"), focusing on their sensitivity towards ethical values as the subjects of AI-aided data collection. As part of this survey, we measured residents' level of concern towards AI-aided collection of their personal data by the *Singapore government* with their reactions towards the same by *businesses*. We also assessed the specific categories of personal data that residents considered important to protect from the government. Our research also provides us with the opportunity to examine differences in the level of concern exhibited by certain demographic groups towards government collection of data categories that are of particular relevance to contact tracing technology.

With this study, we were able to investigate the following research questions:

RQ1. The potential differences between Singapore residents' level of concern with the *Singapore government* as compared to *business* collecting their personal data;
RQ2. The *categories* of personal data that Singapore residents consider important to protect from the Singapore government; and
RQ3. The *relationships* between basic demographic characteristics and Singapore residents' concerns about Singapore government collecting categories of personal data relevant to contact tracing technology.

We note that there have been a number of multi or single country investigations, mainly in the US and European countries, into the attitudes of the public towards the adoption of contact

[27] See, e.g., Alicia Wee and Mark Findlay, "AI and Data Use: Surveillance Technology and Community Disquiet in the Age of COVID-19", Appendix: Google Play Store Reviews of the TraceTogether App (and screenshots) at 9, 52-57.
[28] See discussion in Section II Literature Review for what these categories of data are.
[29] Pouyan Esmaeilzadeh, "Use of AI-based tools for healthcare purposes: a survey study from consumers' perspectives" BMC Medical Informatics and Decision Making (2020) 20:170.

tracing technology and the factors that influence acceptance.[30] On the Singapore front, such studies have been conducted, for example, by the Institute of Policy Studies[31] and YouGov.[32]

By contrast, our study preceded the COVID-19 pandemic and the introduction of tracing technology,[33] and did not purport to elicit responses to questions about the adoption of the technology. Nonetheless, our findings provide a unique perspective on the public's resistance to contact tracing technology, in that it uncovered pre-existing trust concerns and sensitivities among Singapore residents which were subsequently magnified by the chain of events precipitated by the pandemic. In addition, our results could provide more insight into whether the acceptance of contact tracing technology is heavily dependent on context-specific factors such as the COVID-19 emergency and government-mandated measures.

The rest of this chapter is organised as follows: Section II provides a literature review on the linkage between willingness to share information (corresponding to having no or less concern about sharing information) with others, and trust. It also provides the background to our presumption of a difference between responses to AI-aided data collection by government and business in Singapore. In addition, Section II explains the categories of personal data perceived to be placed at risk in the context of contact tracing technology. It also explains our focus on the categories of health history, location and social network information in our analysis of the relationship between certain demographic characteristics and concern about government collection of contact tracing personal data. Section III describes our research methodology while section IV describes our results. In section V, we discuss the implications of our results with respect to Singapore residents' relative trust in government and business concerning contact tracing technology, the categories of personal data that residents considered important to protect from the Singapore government, and the exploratory analyses into certain demographic characteristics and concerns about sharing personal data relevant to contact tracing technology with the Singapore government. Section VI provides some concluding thoughts and implications for government data-collection undertakings, together with suggestions for further research going forward.

II. LITERATURE REVIEW

Willingness to share information as a facet of trust

As mentioned, our survey investigated the level of concern Singapore residents had about collection of particular categories of personal data by the government and a business, respectively, with the underlying premise that a high level of concern would reduce the willingness of residents to share information. This would in turn signal a lower degree of trust reposed in the data-collecting entity. In essence, we define willingness to share information

[30] See, e.g., Genia Kostka and Sabrina Habich-Sobiegalla, 'In Times of Crisis: Public Perceptions Towards COVID-19 Contact Tracing Apps in China, Germany and the US' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3693783 <https://papers.ssrn.com/abstract=3693783> accessed 10 December 2020 and the studies mentioned therein at section "2.2 Public Attitudes of CTAs" (pp 5-6).

[31] Institute of Policy Studies, "Attitudes towards the use of surveillance technologies in the fight against COVID-19" <https://lkyspp.nus.edu.sg/docs/default-source/ips/ips-report-on-attitudes-towards-the-use-of-surveillance-technologies-in-the-fight-against-covid-19-240520.pdf> (accessed 11 October 2020).

[32] See, e.g., "Singaporeans divided on tracking token" (*YouGov*) <https://sg.yougov.com/en-sg/news/2020/06/18/singaporeans-divided-tracking-token/ > accessed 15 December 2020.

[33] We completed gathering the survey responses towards the end of 2019 just as COVID-19 started making its presence known.

with other parties as a facet of trust. Our definition is supported by studies into the construct of trust.

In the context of dyadic relationships within organisations, Mayer, Davis and Schoorman (1995) define trust as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party.”[34] They further note that “making oneself vulnerable” is to take risk and that trust involves a “willingness to take risk”.[35] Usoro *et al.* (2007) helpfully noted that Mayer *et al*’s definition of trust had also been used in non-dyadic and intra-organisational studies.[36] In the context of an individual sharing personal information with an organisation, parallels can usefully be drawn to Mayer *et al*’s definition. When one shares personal information, one places oneself in a position of vulnerability vis-à-vis the recipient of the information, insofar as one takes the risk of what the recipient may do with the information. Thus, willingness to share one’s personal information inevitably involves trust.

Indeed, in the context of the “modern networked life” that is “mediated by information relationships”, Richards and Hartzog (2016) point out that trust is an “essential ingredient” when we share “sensitive personal information with Internet service providers (ISPs), doctors, banks, search engines, credit card companies, and countless other information recipients and intermediaries.”[37] In sharing such information, they note that we trust doctors “not to reveal information about our health and mental state” and “ISPs and search engines not to reveal our search history”.[38]

In addition, studies show a correlation between trust and the individual’s willingness to share personal information with a business.[39] For example, Waldman (2016), in an empirical study of Facebook users, argues that “higher levels of trust in the platform and higher levels of trust in those individuals in our networks are associated with a higher propensity to share personal information” and that “Facebook knows this and it has designed its platform to benefit from it”.[40] More to the point, Waldman noted that “[s]cholars have shown that, with respect to e-commerce websites, higher levels of trust in the website translate into a greater willingness to share”.[41]

[34] Mayer RC, Davis JH and Schoorman FD (1995) ‘An integrative model of organisational trust’, Academy of Management Review 20(3), 709–734 at 712.

[35] Mayer RC, Davis JH and Schoorman FD (1995) ‘An integrative model of organisational trust’, Academy of Management Review 20(3), 709–734 at 712.

[36] Usoro, Abel & Sharratt, Mark & Tsui, Eric & Shekhar, Sandhya. ‘Trust as an antecedent to knowledge sharing in virtual communities of practice’(2007) Knowledge Management Research and Practice. 5. 10.1057/palgrave.kmrp.8500143 at 3-4.

[37] Neil M Richards and Woodrow Hartzog, ‘Taking Trust Seriously in Privacy Law’ (2016) 19 Stanford Technology Law Review 431 at 433.

[38] Neil M Richards and Woodrow Hartzog, ‘Taking Trust Seriously in Privacy Law’ (2016) 19 Stanford Technology Law Review 431 at 460.

[39] See, e.g., Ashish Gupta and Anil Dhami, ‘Measuring the impact of security, trust and privacy in information sharing: A study on social networking sites’ (2015) 17 Journal of Direct, Data and Digital Marketing Practice 43–53; Bomil Suh and Ingoo Han, ‘The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce’ (2003) 7 International Journal of Electronic Commerce 135.

[40] Ari Ezra Waldman, ‘Privacy, Sharing, and Trust: The Facebook Study’ (2016) 67 Case Western Reserve Law Review 193 at 195.

[41] Ari Ezra Waldman, ‘Privacy, Sharing, and Trust: The Facebook Study’ (2016) 67 Case Western Reserve Law Review 193 at 233.

Against this backdrop of trust and its link to the willingness to share personal information, we note that studies generally indicated that the Singapore public reposed a high level of trust in their government. For instance, the World Values Survey Wave 2014 showed that the Singapore government distinguished itself in this regard when compared to other high-income countries: 24% of people in Singapore had a "great deal of confidence" in their government, compared to 5.8% in South Korea, 5.5% in Germany or 3.7% in the US.[42]

Indeed, the Edelman Trust Barometer 2020 (Singapore Report), based on a survey conducted between October and November 2019, indicated that respondents generally trusted the Singapore government. Moreover, compared to the Edelman 2019 Report, trust in the government had risen to 70% from 67% a year ago.[43] Conversely, respondents were neutral in their trust of businesses. In fact, trust in business decreased to 58% from 60% a year ago.[44] Further, in comparison to businesses, the Singapore government was considered more ethical.[45]

In contrast, on a global level, the Edelman Trust Barometer 2020 showed that businesses fared better than governments, with trust at 58% compared to 49%. Even so, there had been a general decline of trust across business sectors, especially in the area of technology, with a 4% reduction from 2019.[46] This could be because, as another study noted, "trust [in technology companies] has been eroding for a while now because of the techlash."[47] Such sentiment was reflected in Amnesty International's observation that "Google and Facebook dominate our modern lives – amassing unparalleled power over the digital world by harvesting and monetising the personal data of billions of people" and that "[t]heir insidious control of our digital lives undermines the very essence of privacy and is one of the defining human rights challenges of our era."[48]

[42]See http://www.worldvaluessurvey.org/WVSOnline.jsp (accessed 31 October 2020). See also Catherine Mei Ling Wong and Olivia Jensen, 'The Paradox of Trust: Perceived Risk and Public Compliance during the COVID-19 Pandemic in Singapore' [2020] Journal of Risk Research 1, 2.

[43] Edelman Trust Barometer 2020 (Singapore) < https://www.edelman.com/sites/g/files/aatuss191/files/2020-06/2020%20Edelman%20Trust%20Barometer%20Singapore%20Report%5b1%5d.pdf>; Shefali Rekhi, 'Trust in Singapore Government up: Edelman Poll' (*The Straits Times*, 22 June 2020) <https://www.straitstimes.com/asia/trust-in-singapore-government-up-edelman-poll> accessed 15 September 2020.

[44] Edelman Trust Barometer 2020 (Singapore) < https://www.edelman.com/sites/g/files/aatuss191/files/2020-06/2020%20Edelman%20Trust%20Barometer%20Singapore%20Report%5b1%5d.pdf>.

[45] Edelman Trust Barometer 2020 (Singapore) < https://www.edelman.com/sites/g/files/aatuss191/files/2020-06/2020%20Edelman%20Trust%20Barometer%20Singapore%20Report%5b1%5d.pdf>.

[46] 2020 Edelman Trust Barometer Global Report (also reported in "Trust in government now exceeds the public's faith in business" (*Quartz* May 2020) <https://qz.com/1851749/covid-19-has-us-trusting-government-more-than-ceos/> (accessed 10 October 2020), and "Trust in business falls behind government" (*Axios* May 2020) <https://www.axios.com/coronavirus-government-trust-business-d045d88d-a3f9-4407-b734-55d51ea0bf69.html>. For some suggestion of a counter-trend in some countries, see The Jakarta Post, 'Why Do We Trust Google More than the Government?' (The Jakarta Post) <https://www.thejakartapost.com/life/2017/11/21/why-do-we-trust-google-more-than-the-government.html> accessed 7 September 2020; Baobao Zhang and Allan Dafoe, 'Artificial Intelligence: American Attitudes and Trends' [2019] SSRN Electronic Journal 20 <https://www.ssrn.com/abstract=3312874> accessed 11 October 2020.

[47] 'Bridging AI's Trust Gaps: Aligning Policymakers and Companies' 15 <https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/ai/ey-bridging-ais-trust-gaps-report.pdf> accessed 17 September 2020. See also Ian I Mitroff and Rune Storesund, Techlash: The Future of the Socially Responsible Tech Organization (Springer International Publishing 2020) at Chapter 1 <http://link.springer.com/10.1007/978-3-030-43279-9> accessed 7 October 2020.

[48] Statement by Kumi Naidoo, Secretary General of Amnesty International in "Amnesty Slams Facebook, Google over 'pervasive Surveillance' Business Model" <https://www.theregister.com/2019/11/21/amnesty_facebook_google/> accessed 15 November 2020).

More relevant to the issue of data collection by business for contact tracing purposes, another study found that "[w]hile technology companies have launched initiatives to track the spread of COVID-19, many consumers are not buying it. 84% of Americans are worried that data collection for COVID-19 containment will sacrifice too much of their privacy, and 74% of Australians say the same."[49] In Singapore, consumers likewise had concerns over businesses' treatment of their personal data. For example, an April 2019 study reported that less than one in four (23%) of Singapore consumers believed that their personal data would be treated in a trustworthy manner by organisations offering digital services.[50]

The foregoing supports the perception that Singapore residents would be more willing to share (or be less concerned about the collection of) their personal data where the entity collecting the information is the Singapore government rather than a business. It also provides the basis for our hypothesis that Singapore residents would be more willing to share contact tracing information with the Singapore government rather than a business.

Personal data perceived to be placed at risk by contact tracing technology

In a survey by Samuel et al (2020) of respondents in France, Germany, Italy, UK and the US in late April 2020, 35% indicated the fear of a contact tracing app rendering the phone vulnerable to hackers as a reason for not installing it.[51] 42% of the respondents also indicated concern about "government surveillance at the end of the epidemic" as a reason for not installing the app.[52]

In Singapore, such fear of surveillance by the government through the use of data collected by the app or token had also been expressed.[53] In addition, the Singapore public were concerned about the possible loss of the collected data to persons hacking into the servers where the data were stored.[54] Despite the Singapore government explanations that the TraceTogether

[49] "The Cost of Privacy" <https://www.okta.com/cost-of-privacy-report/2020/> (accessed 15 November 2020). This was an "online survey of over 12,000 people between the ages of 18 and 75 in six countries: Australia, France, Germany, the Netherlands, the United Kingdom, and the United States."

[50] "Less than 1 in 4 Singapore consumers trust organisations that provide digital services to protect their personal data: Microsoft – IDC Study" <https://news.microsoft.com/en-sg/2019/04/16/less-than-1-in-4-singapore-consumers-trust-organisations-that-provide-digital-services-to-protect-their-personal-data-microsoft-idc-study/> (accessed 11 October 2020).

[51] Samuel Altmann and others, 'Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Evidence' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3590505 <https://papers.ssrn.com/abstract=3590505> accessed 8 December 2020, at p 7.

[52] Samuel Altmann and others, 'Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Evidence' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3590505 <https://papers.ssrn.com/abstract=3590505> accessed 8 December 2020, at p 7.

[53] 'Singapore says 'No' to wearable devices for Covid-19 contact tracing' (*change.org*) <https://www.change.org/p/singapore-government-singapore-says-no-to-wearable-devices-for-covid-19-contact-tracing?fbclid=IwAR23Wqo1tvznlxK9e-xOnUGz99z_ZCitqA9amEfmo5NEewt-YGvtIpiuVJU> accessed 15 December 2020. As of 16 December 2020, the petition had garnered above 54,000 signatures. See also "Coronavirus: why aren't Singapore residents using the TraceTogether contact-tracing app?" (SCMP, 18 May 2020) <https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether> accessed 16 December 2020.

[54] See, for example, Alicia Wee and Mark Findlay, "AI and Data Use: Surveillance Technology and Community Disquiet in the Age of COVID-19", Appendix: Google Play Store Reviews of the TraceTogether App (and screenshots) at p 49. See also "Coronavirus: why aren't Singapore residents using the TraceTogether contact-tracing app?" (SCMP, 18 May 2020) <https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether> accessed 16 December 2020.

technology does not log GPS location data or connect to mobile networks, and hence cannot be used for surveillance of a person's movements,[55] this remains a valid concern:

> "[One] has to acknowledge that the complex software and hardware environment of smartphones with multiple apps makes it more difficult to prevent security issues with smartphone-based contact tracing apps. Also, when it comes to privacy, anonymisation technologies exist, but also here one has to acknowledge that smartphones contain personal information, are always on and as a result their location can be traced."[56]

Thus, as applied to our survey questions, in assessing the level of trust reposed in the government or businesses, we measured the levels of concern about the collection of those categories of personal data that one might find *on a phone*:

- Personal Contact Information
- Work Contact Information
- Credit Card Information
- Demographic Information
- Government Identification
- Health History
- Location
- Purchase History
- Social Network Friends' Information
- Communication History
- Web-surfing History

To assess the particular categories of personal information that the Singapore public considered important to protect from the government, our survey question focused on the same list above.

Certain data categories are of especial relevance to contact tracing technology, given their sensitivity and the perception that they are collected by the technology. These data categories are:

- *Health history*: There could be concern about being stigmatised, or even harassed, if one is infected by COVID-19.[57] In addition, concern over this category of personal data may be more acute given recent incidents in Singapore that resulted in the leak of health-related information. Of note are: (1) the 2018 hacking incident into the database of Singapore's largest group of public healthcare institutions, SingHealth, where 1.5 million patients' particulars (including outpatient dispensed medicines) were stolen;[58] and (2) the 2019 leak of confidential information of HIV-positive individuals (including

[55] https://support.tracetogether.gov.sg/hc/en-sg/articles/360043224874-Can-TraceTogether-track-the-location-of-all-phones-installed-with-the-TraceTogether-App-

[56] European Institute of Information and Technology (a body of the EU) "Anonymous COVID-19 contact tracing using physical tokens" <https://eit.europa.eu/our-activities/covid-19-response/solutions/anonymous-covid-19-contact-tracing-using-physical-tokens> (accessed 26 December 2020).

[57] See, e.g., Sotgiu G, Dobler CC. Social stigma in the time of Coronavirus. Eur Respir J 2020; in press (https://doi.org/10.1183/13993003.02461-2020); "Coronavirus: Social stigma, harassment undermine testing efforts across Asia" (*The Straits Times*) <https://www.straitstimes.com/asia/east-asia/coronavirus-social-stigma-harassment-undermine-testing-efforts-across-asia> accessed 29 December 2020.

[58] 'MOH | News Highlights' <https://www.moh.gov.sg/news-highlights/details/singhealth's-it-system-target-of-cyberattack> accessed 16 December 2020.

their medical information) that was stolen by a fraudster with the aid of his partner who had access to the HIV Registry of the Singapore National Public Health Unit.[59]

- *Social Network Friends' Information*: We took this category of information as a proxy for social contacts' information. The TraceTogether technology captures Bluetooth data of the phones of people in close proximity to the person using the app or token.[60] Naturally, this makes possible the identification of people whom the app or token user spent time with. Yet, there could be people who may wish to keep such information confidential, as for example someone who visited a brothel.[61]
- *Location*: As with the concern to keep the identity of social contacts confidential, people could equally be uncomfortable revealing their location. As mentioned, despite assurances by the government that location data was not collected by the app or token, some members of the Singapore public continued to believe otherwise.[62]

Thus, in assessing the relationship between certain demographic characteristics and the level of concern about government collection of personal data, we narrowed our focus to these data categories.

Relevant demographic factors

The results of existing studies are generally inconclusive as to which individual demographic characteristics affect people's acceptance of technology.[63] For instance, results as to age and gender appear to vary depending on the survey used, as well as the region explored.[64] Few also have studied educational levels, or income levels.[65] As such, our aim is simply to explore whether (and how) such demographic factors would affect acceptance of contact tracing technology in Singapore.

Further, we also explore whether prior computer science or programming experience, or prior exposure to AI would have an impact on willingness to share information. For instance, recent

[59] Data of 14,200 People with HIV Leaked Online by US Fraudster Who Was Deported from Singapore' (The Straits Times, 28 January 2019) <https://www.straitstimes.com/singapore/data-of-14200-singapore-patients-with-hiv-leaked-online-by-american-fraudster-who-was> accessed 16 December 2020.

[60]'How Does the TraceTogether App Work?' (TraceTogether FAQs) <http://support.tracetogether.gov.sg/hc/en-sg/articles/360043543473> accessed 11 September 2020. See also 'How are your possible exposures determined?' (TraceTogether FAQs) <https://support.tracetogether.gov.sg/hc/en-sg/articles/360053464873-How-are-your-possible-exposures-determined-> accessed 16 December 2020.

[61] 'Covid-19: Man in Hong Kong who visited prostitute before testing positive sparks police tracking operation'(*Todayonline*) < https://www.todayonline.com/world/covid-19-man-hong-kong-who-visited-prostitute-testing-positive-sparks-police-tracking> accessed 16 December 2020.

[62] See, for example, "Coronavirus: why aren't Singapore residents using the TraceTogether contact-tracing app?" (SCMP, 18 May 2020) <https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether> accessed 7 October 2020. See, for example, Alicia Wee and Mark Findlay, "AI and Data Use: Surveillance Technology and Community Disquiet in the Age of COVID-19", Appendix: Google Play Store Reviews of the TraceTogether App (and screenshots) at p 51.

[63] Genia Kostka and Sabrina Habich-Sobiegalla, 'In Times of Crisis: Public Perceptions Towards COVID-19 Contact Tracing Apps in China, Germany and the US' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3693783 <https://papers.ssrn.com/abstract=3693783> accessed 10 December 2020.

[64] Genia Kostka and Sabrina Habich-Sobiegalla, 'In Times of Crisis: Public Perceptions Towards COVID-19 Contact Tracing Apps in China, Germany and the US' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3693783 <https://papers.ssrn.com/abstract=3693783> accessed 10 December 2020.

[65] Genia Kostka and Sabrina Habich-Sobiegalla, 'In Times of Crisis: Public Perceptions Towards COVID-19 Contact Tracing Apps in China, Germany and the US' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3693783 <https://papers.ssrn.com/abstract=3693783> accessed 10 December 2020. However, this paper also noted a Pew research center survey which revealed that acceptance is higher among the better educated (Pew Research Center, 2020).

studies in AI adoption in the health-care sector have shown that familiarity with AI could have an impact on a person's intention to use AI technology for health-care purposes.[66] Our expectation is that such prior experience or exposure will be positively correlated with concern about government collection of personal data relevant to contact tracing technology.

III. SURVEY METHODOLOGY

Measures

We carried out this survey in 2019, to determine the attitudes of Singapore residents towards business organisations' use of AI, with a focus on their sensitivity towards ethical values as the subjects of AI-aided data collection.

We based our questions on similar surveys on AI and data collection.[67] We tested out initial versions of the survey questionnaire on two focus groups, one comprising data privacy practitioners (AsiaDPO) and the other comprising academics at an academic forum. We also tested the questionnaire on friends and family, as well as other fellow academics (both in the law discipline and in the social sciences).

We first explored, as between the government and a business, which entity Singapore residents had more trust in (had less concern about) collecting their personal information (RQ1). We then investigated which categories of personal data that residents considered important to protect from the Singapore government as the TraceTogether technology is government-initiated. (RQ2). Finally, we explored the *relationships* between basic demographic characteristics and residents' concerns about the Singapore government collecting personal data relevant to contact tracing technology (RQ3).

To examine RQ1, we asked the survey respondents how concerned they were about the government or a business collecting certain categories of their personal information through the use of AI respectively. The respondents were asked to indicate their level of concern from 1 (*not concerned at all*) to 5 (*extremely concerned*).

To examine RQ2, respondents were asked to select up to 6 categories of personal information they felt were most important to protect from the government.

For each of the questions, the respondents were asked to consider the following categories of personal information:

- Personal Contact Information
- Work Contact Information
- Credit Card Information
- Demographic Information
- Government Identification

[66] Pouyan Esmaeilzadeh, "Use of AI-based tools for healthcare purposes: a survey study from consumers' perspectives" BMC Medical Informatics and Decision Making (2020) 20:170; Songhee Oh; Jae Heon Kim; Sung-Woo Choi; Hee Jeong Lee; Jungrak Hong; & Soon Hyo Kwon, "Physician Confidence in Artificial Intelligence: An Online Mobile Survey" J Med Internet Res 2019;21(3):e12422.

[67] See, e.g., Timothy Morey, Theodore "Theo" Forbath, and Allison Schoop, "Customer Data: Designing for Transparency and Trust" Harvard Business Review May 2015; Global Alliance of Data-Drive Marketing Associations "Global data privacy: What the consumer really thinks" <https://www.acxiom.co.uk/resources/global-data-privacy-what-the-consumer-really-thinks/>.

- Health History
- Location
- Purchase History
- Social Network Friends' Information
- Communication History
- Web-surfing History

To examine RQ3, respondents were asked to answer questions on certain demographic measures, including the typical ones of age, gender, income, and education, as well as prior computer science or programming experience, and exposure to AI. This would allow us to test for associations with concerns about the Singapore government collecting personal data relevant to contact tracing technology.

Participants

A nationally representative sample (in terms of gender, race, and age) of 1001 Singapore residents participated in the study.[68] The respondents comprised 47.55% males and 52.45% females.[69] The race profile of the respondents was: 79.92% Chinese, 10.79% Malay, 5.39% Indian and 3.90% other races.[70] In terms of age, there were 6.69% in the 18-23 range, 33.37% in the 24-39 range, 37.36% in the 40-55 range and 22.58% in the 56 and above range.[71] As our goal was to understand the reactions of all residents, we did not limit our survey to Singapore citizens, but allowed responses from anyone who resided in Singapore.

Procedure

We conducted an online self-administered survey, using a commercial survey company's panel of respondents. The survey company, Qualtrics, drew a random sample from the target population which matched the general demographic percentages of adult residents in Singapore based on gender, age and race. The survey was conducted from late August 2019 to mid-December 2019.

We began the survey with a series of questions relating to AI and data collection, including the questions mentioned above regarding respondents' concern with government and business collecting personal data, as well as the categories of personal data considered important to

[68] Based on a population of approximately 5.7million residents, this meant a confidence level of 99%, 0.5 standard deviation, and approximately 4% margin of error.

[69] Based on data from the Singapore Department of Statistics <https://www.singstat.gov.sg/>, in 2019 males made up 48.91% of the resident population, while females made up 51.09% of the resident population. "Residents" comprises Singapore citizens & permanent residents, while "non-resident" comprises foreigners who were working, studying or living in Singapore but not granted permanent residence, excluding tourists and short-term visitors.

[70] This largely correlates to the 2019 ethnic breakdown of residents in Singapore, based on data from the Singapore Department of Statistics <https://www.singstat.gov.sg/>: "Chinese" 74.36%, "Malays" 13.43%, "Indians" 9.01%, "Others" 3.21%.

[71] The breakdown roughly corresponds to the general breakdown of: Millenials (24-39), Gen-X (40-55), and Boomers (56 - 74). See https://www.pewresearch.org/fact-tank/2020/04/28/millennials-overtake-baby-boomers-as-americas-largest-generation/. The "Boomer" category also roughly corresponds to the Merdeka (61-70) and Pioneer (71 and older) demarcations in Singapore. See https://www.merdekageneration.sg; https://www.pioneers.gov.sg/en-sg/Pages/Home.aspx.
Based on data from the Singapore Department of Statistics <https://www.singstat.gov.sg/>, for the 2019 resident population: those aged 20-24 made up 5.9%; those aged 25-39 made up 31.8%; those aged 40-54 made up 33.9%; and those aged 55 and above made up 26.1%.

protect from the government. At the end of the survey, as mentioned, the respondents completed a number of demographic measures, including the typical ones of age, gender, income, and education, as well as prior computer science or programming experience, and exposure to AI. Table 1 provides a summary of the socio-demographic characteristics of the sample.

IV. RESULTS

RQ1. The potential differences between Singapore residents' level of concern with the Singapore government as compared to business collecting their personal data

First, on average, respondents were at least "moderately concerned" about either the Singapore government or business collecting their data.[72] However, the mean response for *concern about government collecting data* was lower (3.1409) than the mean response for *concern about business collecting data* (3.5441). This suggested a lower level of concern about government collecting personal data than business.

To further explore this potential difference, we conducted 11 Wilcoxon matched pairs signed rank tests for each of the 11 data categories. Table 2 reports the descriptive statistics and Wilcoxon matched pairs signed rank tests (corrected for ties). Based on this test, as compared between the two entities, respondents expressed significantly less concern with the *government* than a *business* collecting personal data.

More specifically, respondents generally expressed significantly less concern with the government than a business collecting the following data categories: personal contact information; work contact information; credit card information; demographic information; government identification; health history; location; social network friends' information; and communication history.[73] We note that there were no significant differences in the median levels of concern with the government than a business collecting respondents' purchase history and web-surfing history.[74]

RQ2. The categories of personal data that Singapore residents consider important to protect from the Singapore government

To further examine the types of information that respondents are most concerned about protecting from the government, respondents were asked to select up to 6 categories of information they felt were most important to protect from the government.

As seen in Table 3, the top three data categories most frequently considered as important to protect from the government were credit card information (65.33%), personal contact

[72] The mean responses for both questions were between "(3) moderately concerned" and "(4) very concerned".

[73] Personal contact information (T = 176786.00, z = -17.32, p < .001); work contact information, (T = 130246.00, z = -12.31, p < .001); credit card information (T = 111052.00, z = -15.02, p < .001); demographic information (T = 42123.5091779.50, z = -7.59, p < .001); government identification (T = 171942.00, z = -17.79, p < .001); health history (T = 27263.501129256.50, z = -13.75, p < .001); location (T = 37010.50106369.50, z = -10.13, p < .001); social network friends' information (T = 45771.0083515.00, z = -5.98, p < .001); and communication history (T = 54241.0084360.00, z = -4.53, p < .001). See results in Table 2.

[74] Collecting purchase history (T = 57880.00, z = -0.60, p = .55); and web-surfing history (T = 65355.50, z = -.15, p = .89). See results in Table 2.

information (45.75%), and communication history (44.86%). The bottom three data categories that were least frequently considered as important to protect from the government were purchase history (26.77%), location (25.17%), and demographic information (20.88%).

RQ3. The relationships between basic demographic characteristics and Singapore residents' concerns about the Singapore government collecting categories of personal data relevant to contact tracing technology

We examined the relationships between a number of demographic characteristics and concern with the government collecting personal data of particular relevance to contact tracing technology.

The socio-demographic characteristics of interest include age, gender, annual household income, educational qualification, self-perceived AI exposure, and prior computing and/or programming experience. To determine relationships between these characteristics (excluding gender) and concern with the government collecting forms of data relevant to contact tracing technologies, namely health history, location, and social network friends' information, we conducted a series of Spearman's rank-order correlations (see Table 4).

We first examined the relationship between age and concern with the government collecting personal information relevant to contact tracing. Spearman's rank-order correlations revealed a significant negative relationship between age and concern with the government collecting health history information. As age of the respondents increased, the less concern they express about government collection of their health history data. However, the analyses also showed that respondents' age was unrelated to their concern with government collection of their location data and social network friends' information.[75]

For the relationship between annual household income[76] and levels of concern, income was positively correlated with concern about the government collecting health history, location, and social network friends' information.[77] Thus higher levels of annual household income were associated with greater concern with the government collecting all three forms of information.

Similarly, educational qualification[78] was positively correlated with concern about the government collecting health history and location data, but unrelated to the collection of social network friends' information.[79] That is, higher educational qualification levels were associated with greater concern about the government collecting health history and location data.

Interestingly, self-perceived exposure to AI was positively correlated to concern with the government collecting health history, location, and social network friends' information.[80] Thus

[75] Health history ($r_s(1001) = -.10, p = .001$); location ($r_s(1001) = .007, p = .83$); social network friends' information ($r_s(1001) = -.013, p = .68$).

[76] Prior to analysis, responses that indicated "Prefer not to say" were excluded.

[77] Health history ($r_s(949) = .099, p = .002$); location ($r_s(949) = .084, p = .009$); social network friends' information ($r_s(949) = .081, p = .012$).

[78] Prior to analysis, responses that indicated post-secondary and diploma and professional qualification were grouped together. Responses that indicated "Others" were also excluded.

[79] Health history ($r_s(963) = .079, p = .015$); location ($r_s(963) = .085, p = .008$); social network friends' information ($r_s(963) = .059, p = .068$).

[80] Health history ($r_s(1001) = .083, p = .009$); location ($r_s(1001) = .11, p < .001$); social network friends' information ($r_s(1001) = .13, p < .001$).

the more exposed to AI the respondents perceived themselves to be, the greater concern they expressed about the government collecting all three forms of information.

Analyses also showed that prior computing and/or programming experience was positively correlated with concern about the government collecting social network friends' information but not with collecting health history and location data.[81] This suggests that respondents with prior computing and/or programming experience were more likely to express concern with the government collecting social network friends' information than respondents without such prior experience.

Finally, to explore potential gender differences regarding concern with the government collecting these three forms of information, we conducted Mann-Whitney *U* tests. Figures 1, 2, and 3 illustrate gender differences in the concern about the government collecting health history, location, and social network friends' information respectively.

The analyses revealed no significant difference between male and female respondents in their concern about the government collecting health history[82] or location data.[83] However, male respondents expressed significantly greater concern than female respondents about the government collecting social network friends' information.[84]

V. DISCUSSION

We had defined the willingness to share information as a facet of trust, and hypothesised that given the general perception that Singapore residents trusted their government more than businesses, they would be more willing to share contact tracing information with the former rather than the latter.

At a general level, our results support our hypothesis above. With regard to RQ1 (the differences between Singaporean residents' level of concern with the Singapore government as compared to business collecting their personal data), the results show that Singapore residents were less concerned about the government, relative to a business, engaging in collection of most categories of personal data which were perceived to be placed at risk by contact tracing technology.

However, as had been noted, the reality on the ground is that some Singapore residents are reluctant to download the TraceTogether app or to use the TraceTogether token, even before the January 2021 revelation. Our results show certain trends that could account for this phenomenon. Specifically, the results for RQ3 (the relationships between basic demographic characteristics and concerns pertaining to Singapore government collecting personal data relevant to contact tracing technology) suggest that the higher a person's income and education, the more concerned he or she would be with the government collecting such data. The results

[81] Social network friends' information ($r_s(1001) = .094$, $p = .003$); health history ($r_s(1001) = .057$, $p = .071$); location ($r_s(1001) = .059$, $p = .062$).

[82] Male respondents (*Mean Rank* = 506.28, *n* = 476) compared to female respondents (*Mean Rank* = 496.21, *n* = 525), *U* = 122435.00, *z* = -0.56 (corrected for ties), *p* = .57.

[83] Male respondents (*Mean Rank* = 513.25, *n* = 476) compared to female respondents (*Mean Rank* = 489.89, *n* = 525), *U* = 119119.00, *z* = -1.31(corrected for ties), *p* = .19.

[84] Male respondents (*Mean Rank* = 521.99, *n* = 476) compared to female respondents (*Mean Rank* = 481.97, *n* = 525), *U* = 114959.00, *z* = -2.25 (corrected for ties), *p* = .025.

further suggest that the greater a person's self-perceived exposure to AI, the more concerned he or she would be with the government collecting such data.

In total, this suggests that residents inhabiting such demographics may be more resistant to sharing contact tracing data with the Singapore government. Thus, although our results support our hypothesis at a general level, they also provided insights into why there may be segments of the Singapore public that would resist adopting contact tracing technology.

We note that data on health history (29.97%), location (25.17%) and social network friends' information (40.66%) are not within the top three categories considered important to protect from the government. Nevertheless, the percentages of Singapore residents who considered them important to protect were certainly not insignificant. In fact, our results show that concern to protect each of the 11 categories of personal data from the Singapore government existed even in pre-COVID times.

Indeed, Singapore residents were already "moderately concerned" about the government engaging in AI-aided collection of their personal data before the advent of COVID-19 and the use of AI-assisted contact tracing technology. It is thus not too far-fetched to surmise that the level of concern would only rise when privacy-compromising technology is deployed, especially when there is a prospect that its use could become the new normal in even post-pandemic times.[85] Further reasons that could account for the resistance to the TraceTogether technology are:

- residents' data security concerns, given that there had been massive data breaches into government online portals in the recent past;[86]
- policymakers, in the face of the pandemic, treating "…civil liberties and data integrity [as] the necessary casualties of policies for a safer society";[87]
- the above phenomenon, in turn, could have triggered visceral fears of a surveillance government, as is evident from an online petition that declared: "All that is stopping the Singapore government from becoming a surveillance state is the advent and mandating the compulsory usage of such a wearable device, …What comes next would be laws that state these devices must not be turned off [and must] remain on a person at all times - thus sealing our fate as a police state";[88] and
- the fact that such fears are naturally fed "…in times of a pandemic (when surveillance is more obvious and apparent than traditional citizen monitoring devices) [providing] a

[85] Marina Motsenok and others, 'The Slippery Slope of Rights-Restricting Temporary Measures: An Experimental Analysis' [2020] Behavioural Public Policy 1.

[86] In 2019 alone, there were three high profile data breaches, see: 'SINGAPORE — The Personal Data of More than 808,000 Blood Donors Ended up on the Internet in January — and Was Left There for Nine Weeks — by a Vendor of the Health Sciences Authority (HSA), the Authorities Said on Friday (March 15).' (*TODAYonline*) 8 <https://www.todayonline.com/singapore/personal-data-808000-blood-donors-compromised-nine-weeks-hsa-lodges-police-report> accessed 15 November 2020.; 'Data of 14,200 People with HIV Leaked Online by US Fraudster Who Was Deported from Singapore' (*The Straits Times*, 28 January 2019) <https://www.straitstimes.com/singapore/data-of-14200-singapore-patients-with-hiv-leaked-online-by-american-fraudster-who-was> accessed 15 November 2020.; 'Passwords and Usernames of Staff from MOH, MOE and Other Agencies Stolen and Put up for Sale by Hackers' (*The Straits Times*, 21 March 2019) <https://www.straitstimes.com/singapore/compromised-log-ins-passwords-from-several-govt-agencies-on-sale-online-says-russian-cyber> accessed 15 November 2020.

[87] Alicia Wee and Mark Findlay, "AI and Data Use: Surveillance Technology and Community Disquiet in the Age of COVID-19", at p 4.

[88] "TraceTogether: Singapore turns to wearable contact-tracing Covid tech" (*BBC* July 2020) <https://www.bbc.com/news/technology-53146360> (accessed 11 October 2020).

> regular reminder that individuals are being tracked, logged, and aggregated in mass data-sharing practices like never before."[89]

And the fears could be well-founded. An expert had noted that the data collected by the TraceTogether tokens would allow the "Ministry of Health" to "go from this cryptic, secret number that only they know, to a phone number - to an individual".[90] Even if such fears may be overhyped, it is worth reiterating that in such situations, the public's perception of the technology and how it may operate would likely have greater impact on their actions.[91]
We note that the results do not necessarily imply acceptance of the Apple and Google technology, even though it offers greater privacy and autonomy to the user. As mentioned, our results show an overarching tendency for Singapore residents to be more wary of businesses collecting their personal data, including the three data categories of particular relevance to contact tracing technology.

Limitations

As the respondents are Singapore residents, the results may not be generalisable beyond the Singapore context. Additionally, while large sample sizes generally result in more precise estimates of population characteristics, they may also over-emphasise certain effects.[92] Finally, the usual limitations of an online and self-administered survey would also apply here.[93] However, to the extent practicable, we ensured that the respondents generally represented Singapore residents, in terms of age, gender, and race. The largely demographic representation of the respondents should therefore have ameliorated those problems. [94]

VI. CONCLUSION

Although our survey was conducted before the onslaught of COVID-19 and the accompanying use of privacy-compromising contact tracing technology, our findings still served to provide insights into the resistance towards the use of such technology. In particular, our findings show that there already existed concerns about government collection of personal data and corresponding trust issues before they became magnified by subsequent events. To this extent, it may be inferred that the high adoption rate[95] of the TraceTogether technology by Singapore residents at this point in time is a context-specific phenomenon, driven by the COVID-19

[89] Alicia Wee and Mark Findlay, "AI and Data Use: Surveillance Technology and Community Disquiet in the Age of COVID-19", at p 6.

[90] Statement of hardware developer Mr Sean Cross, see "TraceTogether: Singapore turns to wearable contact-tracing Covid tech" (BBC July 2020) <https://www.bbc.com/news/technology-53146360> (accessed 11 October 2020).

[91] This is also supported by the idea that public trust is often perceptual and subjective rather than objective in nature. See Nye, J., Jr. 1997. Introduction: The decline of confidence in government. In Why people don't trust government, ed. J. Nye Jr., P. Zelikow, and D. King, pp. 1–18. Cambridge, MA: Harvard University Press cited in EW Welch, 'Linking Citizen Satisfaction with E-Government and Trust in Government' (2004) 15 Journal of Public Administration Research and Theory 371, 374.

[92] Bjorn Lantz, "The large sample size fallacy" (2013) Scandinavian Journal of Caring Sciences, 487-492.

[93] See Mike McConville & Wing Hong Chui "Introduction and Overview", in Mike McConville & Wing Hong Chui, *Research Methods for Law* (Edinburgh University Press, 2007) at p83; Jelke Bethlehem "Selection Bias in Web Surveys" (2010) 78(2) International Statistical Review 161–188.

[94] See also Joel R. Evans, Anil Mathur "The Value of Online Surveys" (2005) 15(2) Internet Research 195-219 for a discussion of some of the positive aspects of conducting surveys online.

[95] "Budget debate: Contact tracing process shortened with almost 90% of S'pore residents using TraceTogether" (*Straits Times*, 26 February 2021) <https://www.straitstimes.com/singapore/politics/almost-90-per-cent-of-residents-on-tracetogether-programme> (accessed 11 March 2021).

emergency and government-mandated measures. Once the emergency is over, it may well be that Singapore residents will revert to at least their pre-COVID-19 levels, if not higher levels of concern over the government's collection of personal data given the January 2021 revelation. Indeed, the public outcry that followed the revelation was immediate. Some residents experienced a "visceral feeling of betrayal" and expressed their unhappiness and fear as follows:

> "If you have the realisation that (the data) would not be as private as you mentioned earlier, why didn't you say something? … It does feel like there has been a promise broken... It feels like choosing not to use TraceTogether — and to use only the other (SafeEntry system) — is the least I can do to assuage my emotions."[96]
>
> "It's kind of like the start of your worst fears happening, and it may unravel further."

Other residents have raised concerns about a breach of trust[97] including what was seen as a "bait-and-switch" by the government.[98] While the government quickly passed legislation restricting the use of contact tracing data in criminal investigations to only serious crimes (such as murder and terrorism), along with certain other data protection safeguards,[99] it is uncertain if the concerns have been assuaged.

The results of our study and this turn of events should give the Singapore government pause as there are wider implications at stake beyond the acceptance of contact tracing technology. The current efforts to make Singapore an AI hub and smart nation[100] would naturally involve the need to collect large amounts of data from the population. As it is, our study shows that increased exposure to AI correlates to having greater concern about sharing personal data with the government. This implies that Singapore's push towards a more AI-savvy population[101] could simultaneously hinder its AI hub ambitions. The public disquiet highlighted above also indicates that maintaining trust is vital for the success of any government-initiative, even ones that are intended for the public good. The Singapore government would do well to heed the expressed sentiments on the ground in its push towards making Singapore a smart nation – whether the endeavour would be a smooth or rocky one would depend on this, as the experience with getting Singapore residents to adopt the TraceTogether technology has amply shown.

[96] "Some TraceTogether users upset with Govt's revelation on police access to data, say they'll use it less" (*Today*, Jan 7 2021) <https://www.todayonline.com/singapore/some-tracetogether-users-upset-govts-revelation-police-access-data-say-theyll-use-it-less?cid=emarsys-today_TODAY%27s%20morning%20briefing%20for%20Jan%207,%202021%20%28ACTIVE%29_newsletter_07012021_today> (accessed 24 February 2021).

[97] See, e.g., "Netizen vents frustration against TraceTogether in profanity-filled post" <https://theindependent.sg/netizen-vents-frustration-against-tracetogether-in-profanity-filled-post/> (accessed 24 February 2021).

[98] "Broken promises: How Singapore lost trust on contact tracing privacy" (*MIT Technology Review*, January 11 2021) <https://www.technologyreview.com/2021/01/11/1016004/singapore-tracetogether-contact-tracing-police/> (24 February 2021).

[99] "Bill limiting police use of TraceTogether data to serious crimes passed" (*Straits Times*, 2 February 2021) <https://www.straitstimes.com/singapore/politics/bill-limiting-use-of-tracetogether-for-serious-crimes-passed-with-govt-assurances> (accessed 24 February 2021).

[100] See, e.g., the Smart Nation Open Data Portal <https://www.smartnation.gov.sg/resources/open-data-resources> (accessed 28 December 2020). See also the recent amendments to the Personal Data Protection Act 2012 in Bill No. 37/2020, which was passed by Parliament in November 2020, which allowed for new exceptions under which a business can collect, use and disclose personal data about an individual without said individual's consent.

[101] See, e.g, National Artificial Intelligence Strategy <https://www.smartnation.gov.sg/docs/default-source/default-document-library/national-ai-strategy.pdf?sfvrsn=2c3bd8e9_4> (accessed 30 December 2020).

Going forward, it would be of interest to follow up our results with further research into residents' responses after the COVID-19 situation has been resolved, to determine the changes, if any, in residents' attitudes towards data collection by the government, and the factors that contribute to such changes. Deeper investigations could also be made into the socio-demographic factors that correlate with or would foster trust in government data collection.

Tables

Table 1. Summary of the key socio-demographic characteristics of the sample.

Gender		Frequency	%
	Male	476	47.55%
	Female	525	52.45%
Age (years)			
	18-23 (Youth)	67	6.69%
	24-39 (Millenial)	334	33.37%
	40-55 (Gen X)	374	37.36%
	56-74 (Boomer)	216	21.6%
	75 and above (Elder)	10	1.0%
Race			
	Chinese	800	79.92%
	Malay	108	10.79%
	Indian	54	5.39%
	Others	39	3.90%
Income			
	$0	9	0.90%
	Less than $24,999	72	7.19%
	$25,000 to $49,999	139	13.89%
	$50,000 to $74,999	165	16.48%
	$75,000 to $99,999	155	15.48%
	$100,000 to $124,999	159	15.88%
	$125,000 to $149,999	73	7.29%
	$150,000 to $174,999	47	4.70%
	$175,000 to $200,000	49	4.90%
	$200,000 or higher	81	8.09%
	Prefer not to say	52	5.19%
Education			
	Primary (i.e. PSLE and below)	8	0.80%
	Secondary (i.e. GCE “O”/ “N” Levels)	106	10.59%
	Post Secondary (Non-Tertiary, i.e. ITE, JC)	70	6.99%
	Diploma & Professional Qualification (i.e. Polytechnic and similar)	202	20.18%
	University Degree (i.e. Bachelor’s or Equivalent)	438	43.76%
	Postgraduate - Masters (or Equivalent)	139	13.89%
	Postgraduate - Doctorate (or Equivalent)	36	3.60%
	Others	2	0.20%
Prior computer science/programming experience			
	No	653	65.23%
	Yes	348	34.77%

Self-perceived exposure to AI			
	None at all	29	2.9%
	A little	334	33.4%
	A moderate amount	443	44.3%
	A lot	195	19.5%

Table 2. Descriptive statistics and Wilcoxon matched pairs signed rank tests for the concern with the government and a business collecting personal information for each data category.

	Median		Mean Rank		Sum of Ranks			
	Government	Business	Negative	Positive	Negative	Positive	*Z*	*p*-value
Personal Contact Information	3.00	4.00	213.39	335.46	21979.00	176786.00	-17.32[a]	<.001[***]
Work Contact Information	3.00	3.00	245.51	302.19	35354.00	130246.00	-12.31[a]	<.001[***]
Credit Card Information	4.00	5.00	191.51	263.78	15704.00	111052.00	-15.0 2[a]	<.001[***]
Demographic Information	3.00	3.00	234.02	272.34	42123.50	91779.50	-7.59[a]	<.001[***]
Government Identification	3.00	4.00	174.78	333.87	17478.00	171942.00	-17.78[a]	<.001[***]
Health History	3.00	4.00	216.38	298.51	27263.50	129256.50	-13.75[a]	<.001[***]
Location	3.00	3.00	229.88	284.41	37010.50	106369.50	-10.13[a]	<.001[***]
Purchase History	3.00	3.00	245.25	243.79	57880.00	61436.00	-0.60[a]	.55
Social Network Friends' Information	3.00	3.00	232.34	268.54	45771.00	83515.00	-5.98[a]	<.001[***]
Communication History	3.00	4.00	251.12	272.13	54241.00	84360.00	-4.53[a]	<.001[***]
Web-surfing History	3.00	3.00	254.30	255.71	65355.50	64439.50	-0.14[b]	.89

[a] Based on negative ranks.
[b] Based on positive ranks.
[**] *p*-value ≤ .05.
[**] *p*-value ≤ .01.
[***] *p*-value ≤ .001.

Table 3. Frequency and percentage of respondents that selected a category of information as important to protect from the government.

	Frequency	%
Credit Card Information[a]	654	65.33%
Personal Contact Information[a]	458	45.75%
Communication History[a]	449	44.86%
Social Network Friends' Information	407	40.66%
Government Identification	391	39.06%
Web-surfing History	365	36.46%
Health History	300	29.97%
Work Contact Information	292	29.17%
Purchase History[b]	268	26.77%
Location[b]	252	25.17%
Demographic Information[b]	209	20.88%

[a] Top three categories of information considered as important to protect from the government.

[b] Bottom three categories of information considered as important to protect from the government.

Table 4. Spearman correlations for concern with the government collecting personal information pertaining to health history, location, and social network friends' information with selected socio-demographic variables.

			Concern with the Government Collecting Personal Information Pertaining to		
Socio-demographic Variable	N		Health History	Location	Social Network Friends' Information
1. Age	1001	Spearman's Rho	.007	-.10***	-.013
		p-value	(.83)	(.001)	(.68)
2. Annual Household Income	949	Spearman's Rho	.099**	.084**	.081*
		p-value	(.002)	(.009)	(.012)
3. Educational Qualification	963	Spearman's Rho	.079*	.085**	.059
		p-value	(.015)	(.008)	(.068)
4. Self-perceived AI Exposure	1001	Spearman's Rho	.083**	.11***	.13***
		p-value	(.009)	(<.001)	(<.001)
5. Prior Computing and/or Programming Experience (1=No, 2=Yes)	1001	Spearman's Rho	.057	.059	.094**
		p-value	(.071)	(.062)	(.003)

Figures

Figure 1. The distribution of males' (*n* = 476) and females' (*n* = 525) concern with the government collecting health history information.

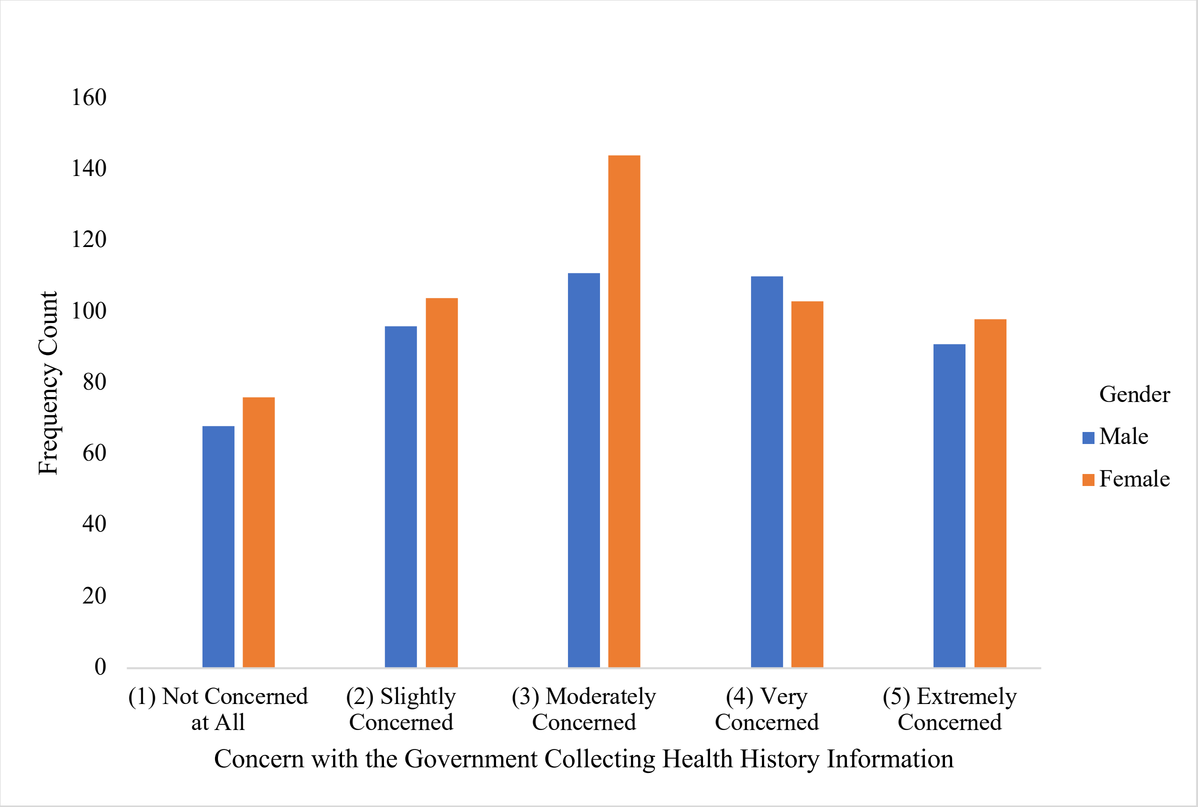


Figure 2. The distribution of males' (*n* = 476) and females' (*n* = 525) concern with the government collecting location information.

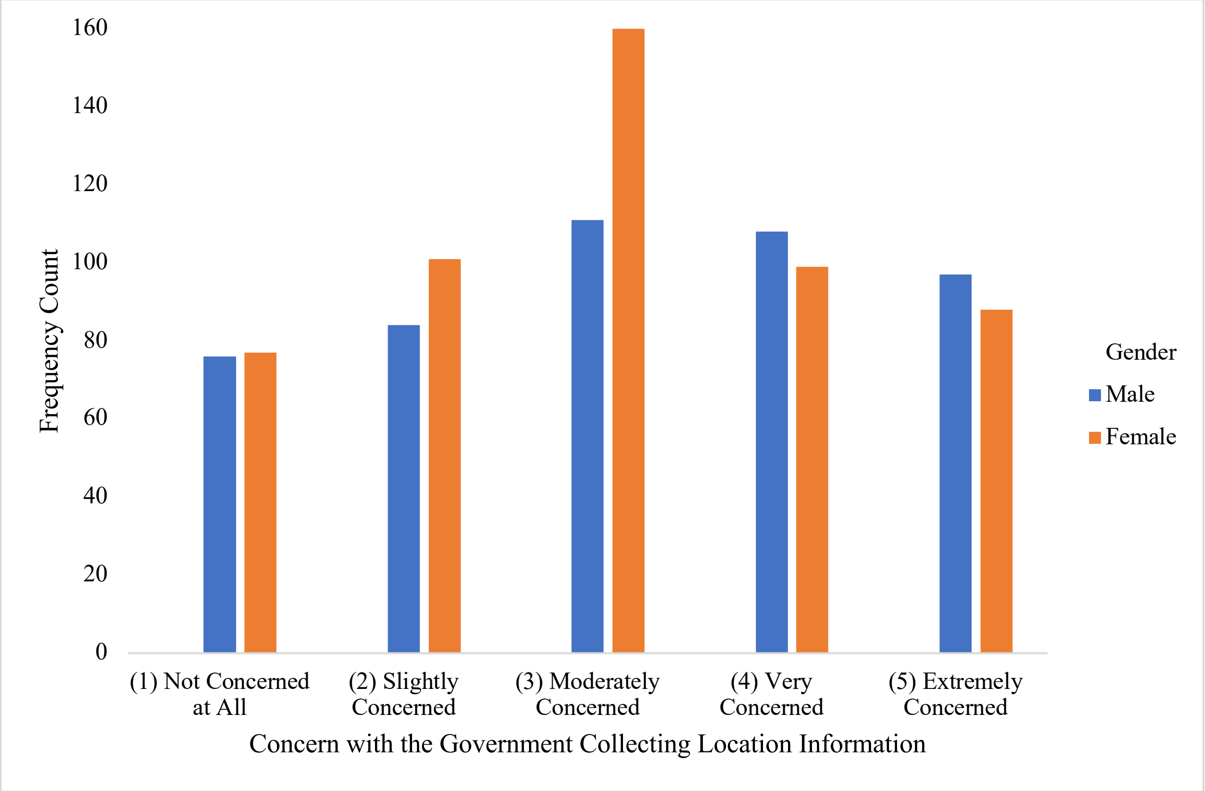
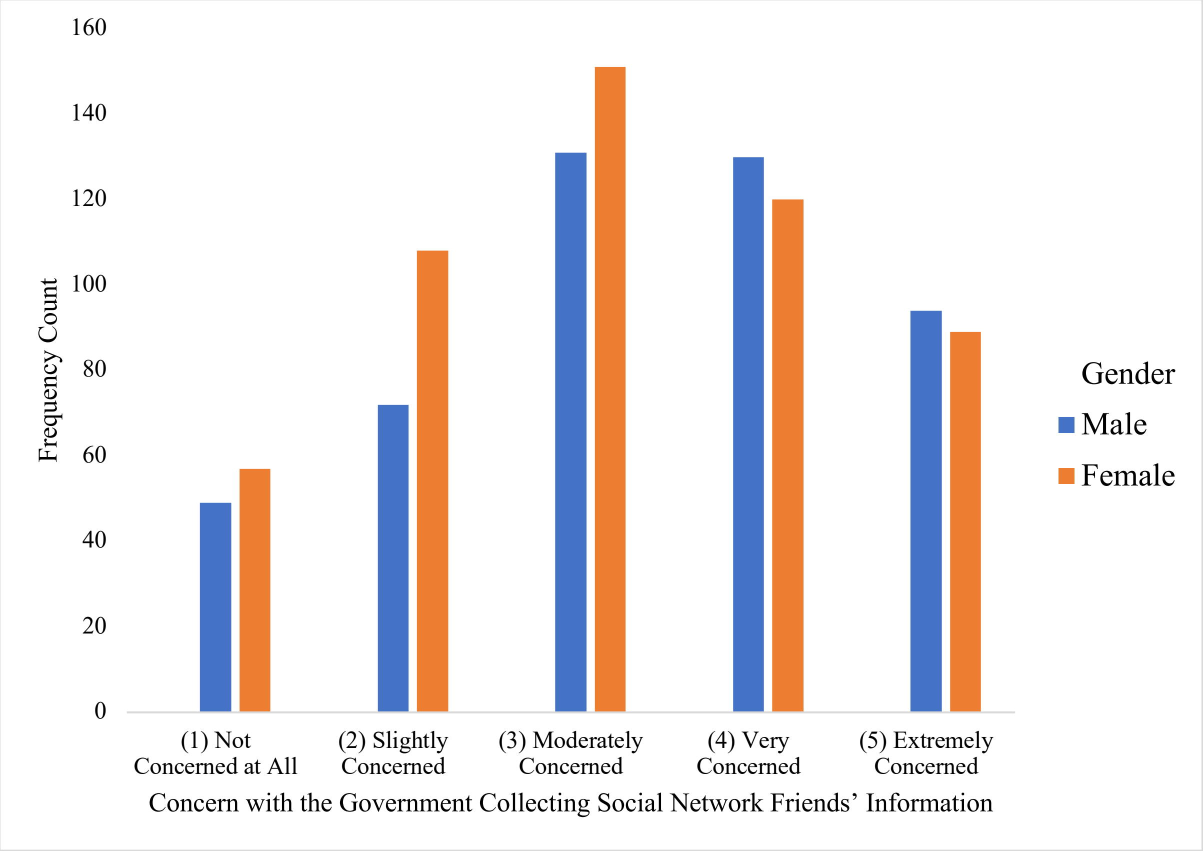


Figure 3. The distribution of males' (*n* = 476) and females' (*n* = 525) concern with the government collecting social network friends' information.


Frequency Count
(1) Not Concerned at All
(2) Slightly Concerned
(3) Moderately Concerned
(4) Very Concerned
(5) Extremely Concerned
Concern with the Government Collecting Social Network Friends' Information
Gender
Male
Female