2021

Investigating the role of Personal Responsibility in safeguarding Privacy in Online Engagements

STEP0012 REA ASSESSMENT

19149973

Executive Summary

Background

The global Internet penetration rate has steadily risen since 2005[1] and is predicted to increase to 70% by 2023[2]. By 2025[3], over 4 billion people globally are also projected to use social media. Trends like participatory social media challenges spur its users to share personal information[4,5], sometimes inadvertently, on these platforms. Congruent with these advancements is the spate of privacy-related breaches such as the harvesting of user data by Cambridge Analytica to allegedly influence voter sentiment in the 2016 Brexit referendum and United States (US) presidential elections[6]. In view of this background, there is a need to investigate if personal responsibility influences individuals in safeguarding their privacy in online environments including social networking sites (SNSs) and the Internet in general.

Research Questions

This rapid evidence assessment (REA) aims to answer the research question; *'what evidence exists to show that personal responsibility plays a role in users safeguarding their privacy in online environments/digital platforms?'* Three sub-questions are also defined as follows:

- To what extent does personal responsibility inform user behaviour in protecting their privacy on digital platforms?
- What factors aid users in proactively protecting their privacy on digital platforms?
- How effective are these factors in influencing users to be responsible for their privacy on digital platforms?

Objectives

By systematically reviewing existing research, this assessment would explore the extent to which personal responsibility informs individuals in protecting their privacy on digital platforms. It also seeks to identify possible factors that influence individuals to proactively protect their privacy online. As Internet penetration grows, the findings would be relevant to help new Internet entrants safely navigate online platforms. Additionally, insights surfaced from the review may present the opportunity for further research in the digital literacy and data privacy awareness domains.

Methods

Guided by a protocol, the search focused on three multidisciplinary databases. Any study discussing user privacy behaviour on digital platforms that employed a range of research methodologies (qualitative, quantitative, mixed methods and evidence reviews) was included. Studies that were Medical or Business-related, not peer-reviewed, not in English and not at final publication stage were excluded. 50 studies satisfied the inclusion criteria for full-text screening, from which a final 21 studies were selected for review and synthesis.

Findings and conclusion

The REA surfaced evidence that has considered the role of personal responsibility in helping individuals to protect their privacy online. Although the evidence highlights its importance, personal responsibility alone cannot improve user attitudes toward preserving their privacy. Rather, a multi-pronged approach comprising personalised nudging/awareness programmes and redesigned privacy controls on SNSs is advised. The REA also identifies possible avenues for future research on other SNSs besides Facebook which was the predominantly assessed platform. Furthermore, as over 60% of the studies assessed for this REA presents a US context, it would be relevant to conduct research that are salient to other parts of the world.

Introduction

A significant invention of the 20th century, the Internet is acknowledged as being instrumental to providing a breadth of benefits including access to information, seamless communication, facilitating commercial activity and building and preserving social interactions[7]. The Internet's open and generative structure[8] has also resulted in the creation of social media platforms like Facebook and Twitter. Described by Carr & Hayes as "Internet-based channels that allow users to opportunistically interact and selectively self-present"[9], these platforms or social networking sites (SNSs) enable their users to communicate and share information, almost unfettered, either about themselves or their associates[10,11]. Popular among diverse age and population groups, these sites are also depended on for creating wider social connections beyond individual local communities[12].

Although the positive impacts of the Internet and its associative technologies are broadly evident, privacy breaches have however been steadily increasing in recent years. In 2017, over 90 million user accounts on a DNA testing service were compromised leading to the exposure of users' emails and hashed passwords[13]. While this breach did not reveal sensitive information, the 2015 data leaks on a controversial online dating service resulted in the disclosure of private information including the names, home and email addresses, and sexual preferences of 33 million subscribed users[14]. Not only did this experience prove embarrassing for its users, in some instances it was also potentially dangerous for subscribers living in conservative societies[15]. Perhaps one of the more concerning information leakages is the case of Cambridge Analytica acquiring user responses to a personality test application hosted on Facebook[16]. The company allegedly manipulated this sensitive data to influence voter sentiment in the 2016 Brexit referendum and United States presidential elections.[6] Considering that this data was mostly user-generated, a consumer protection expert has described individuals as "shar[ing] too much and think[ing] too little"[17] in relation to social media use. Such is the prevalence of this sharing phenomenon that the term "sharenting" has been coined to explain the propensity of parents and child-minders to publish personal information including photographs of children online[18]. In this way, parents unwittingly breach children's privacy long before they are able to consent to their data being shared online. While research into the different facets of sharenting is still ongoing, it has been suggested that improved digital literacy skills could lead individuals to be more aware of their privacy as they navigate online platforms[18,19]. The spill-over effects of sharing are however not restricted to the parent-child dynamic alone. In their paper, Kekulluoglu et al centre their research on designing a model to prevent privacy breaches that could arise from individuals posting photographs or content containing details of their friends or connections on SNSs[10]. An element that significantly compounds these unintended disclosures is the viral nature of SNSs that results in personal information being viewed by unwanted parties; a concern which could expose individuals to dangers like paedophiles or cyber-stalkers[20].

In view of these issues, this study intends to investigate the role of personal responsibility in enabling individuals manage their privacy more proactively on the Internet and social networking sites. With global Internet diffusion rates estimated to grow to 70% by 2023[2], the outcome of this synthesis could be a valuable input to digital literacy programmes targeted at empowering individuals to protect their privacy more proactively as they use online services. There is also the opportunity to identify potential research pathways in the digital literacy and data privacy awareness domains.

Study objectives

The systematic assessment seeks to understand if personal responsibility as a behavioural trait, compels individuals to protect their privacy while online, by answering this overarching research question:

- *What evidence exists to show that personal responsibility plays a role in users safeguarding their privacy in online environments (digital platforms including the Internet and social network sites)?*

Three sub-research questions have also been defined to contextualise the main research question, as well as to understand specific elements in the existing research that would lead to a reasonable conclusion:

a) *To what extent does personal responsibility influence user behaviour in protecting privacy on digital platforms?*
Sub-question a aims to understand if an awareness of online privacy risks impacts individuals' agency to use the Internet and social network sites in a way that preserves their privacy.

b) *What factors aid users in proactively protecting their privacy on digital platforms?*
Sub-question b aims to identify the underlying factors that contribute to an improved understanding of existing privacy risks online, and how they are employed by users to navigate these platforms more safely.

c) *How effective are these factors in influencing users to be responsible for their privacy on digital platforms?*
Sub-question c is intended to provide information on the effectiveness of the factors identified in b above and uncover possible reasons behind this. It would also signal existing limitations of these factors which may be relevant for future research or further investigation.

Given that individuals actively and voluntarily publish information on digital platforms that may be leaked via privacy breaches, this assessment focuses on reviewing existing evidence of elements which lead individuals to be proactive in protecting their privacy online. Conversely, an understanding of current reasons for users not being more involved in preserving their privacy is also of interest to this study. In addition, the study is concerned with determining if personal responsibility is sufficient to inform better user choices and probable factors that prevent individuals from exercising this personal responsibility. Finally, this assessment seeks to identify an evidence base that would enhance ongoing digital literacy efforts to cater for future Internet users.

Methodology

Overview

A protocol was designed to guide the rapid evidence assessment (REA) conducted for this study. The inclusion and exclusion criteria, search strategy, screening process and for this assessment are summarised in the sections below. Full details of these elements are outlined in the guidance protocol in Annex 1.

Inclusion and Exclusion Criteria

Studies were selected if they satisfied the terms below:

- from 2010 to date (2021)
- using a range of methodologies including qualitative, quantitative (including experiments), mixed methods, case studies, and other evidence reviews
- indicating user interactions with digital platforms including social media and the Internet in general
- discussing user behaviours and attitudes to privacy on digital platforms

On the other hand, the following exclusion criteria were applied on the search:

- not peer-reviewed
- not at the final stage
- publications not available in English due to the researcher's primary language skills being English and limited resources available for the review
- Medical Science related papers as their focus centres on medical ethics like secure management/disclosure of patient information, which does not fully address the research question(s).
- Business, Management and Accounting related studies because they address privacy concerns through the lenses of firms and markets and not the individual.

Search strategy and databases

The search was systematically conducted on three electronic databases – ProQuest, Scopus and Web of Science. All three databases provide access to studies from a multidisciplinary base. ProQuest provides multidisciplinary research material including science and technology studies and the social sciences. An interdisciplinarity database, Scopus contains studies from social sciences, physical sciences, health sciences, and life sciences subject areas. Web of Science provides scholarly material from subject areas including social sciences, sciences, and the humanities.

The search was conducted using terms constructed from four concepts in the main research question and some elements of the sub-questions. Concept 1 (Evidence) was to focus the search on studies that apply varied methods, while concepts 2 – 4 were intended to retrieve results that cater directly to the problem and main research question. To return a relatively high relevance of results, queries were built for each concept and then combined to arrive at a final search query. Afterwards, the search query was applied in the databases, with the only difference being variations in the syntax recognised by each database. The searches were conducted at the abstract, title and keywords levels.

Table 1: *Database Search Concepts*

Concept 1: Evidence	**Concept 2:** Personal Responsibility	**Concept 3:** Privacy	**Concept 4:** Online
meta-analy* OR "systematic review" OR (design or study or analysis) OR intervention* OR ("quasi experiment*" or "quasi-experiment*")	(user NEAR/3 responsibility) OR (consumer NEAR/3 responsibility) OR (citizen NEAR/3 responsibility) OR (personal NEAR/3 responsibility) OR (individual NEAR/3 responsibility) OR (user NEAR/3 accountability) OR (consumer NEAR/3 accountability) OR (citizen NEAR/3 accountability) OR (personal NEAR/3 accountability) OR (individual NEAR/3 accountability)	privacy OR secur* OR safe* OR protect* OR private	(social NEAR/3 media) OR ("online social network*") OR (social NEAR/3 networking NEAR/3 site*) OR ("online platform*") OR ("digital platform*") OR (internet) OR (cyber)

Concept 1: Evidence	**Concept 2:** Personal Responsibility	**Concept 3:** Privacy	**Concept 4:** Online
OR experiment*	OR (user NEAR/3 agenc*) OR (consumer NEAR/3 agenc*) OR (citizen NEAR/3 agenc*) OR (personal NEAR/3 agenc*) OR (individual NEAR/3 agenc*) OR (self-censor*) OR ("self censor*") OR (self NEAR/3 censor*)		

Screening

Screening proceeded with applying subject area, period and language filters on the 434 results returned from the search which yielded 239 studies. A duplicates check excluded 60 studies leaving 179 results. Next, studies with abstracts that fully or partially met the inclusion criteria and contained any of the search terms or concepts were read in full while those not satisfying any of the criteria were excluded from further review. It was necessary to include partly compliant studies to ensure enough data was captured and prevent unintentional omissions which could be relevant to this study.

Summary results of search and relevant studies extraction

129 studies were excluded after the abstract level screening. The 50 studies left were then screened at full text to ascertain the extent to which they addressed the main research question as well as the sub-questions. A decision tree and evidence appraisal scheme (see protocol in Annex 1) were applied to arrive at the final 15 studies which form the basis of this REA. Excluded studies comprised e-government, ethical use of social media and cloud technology topics.

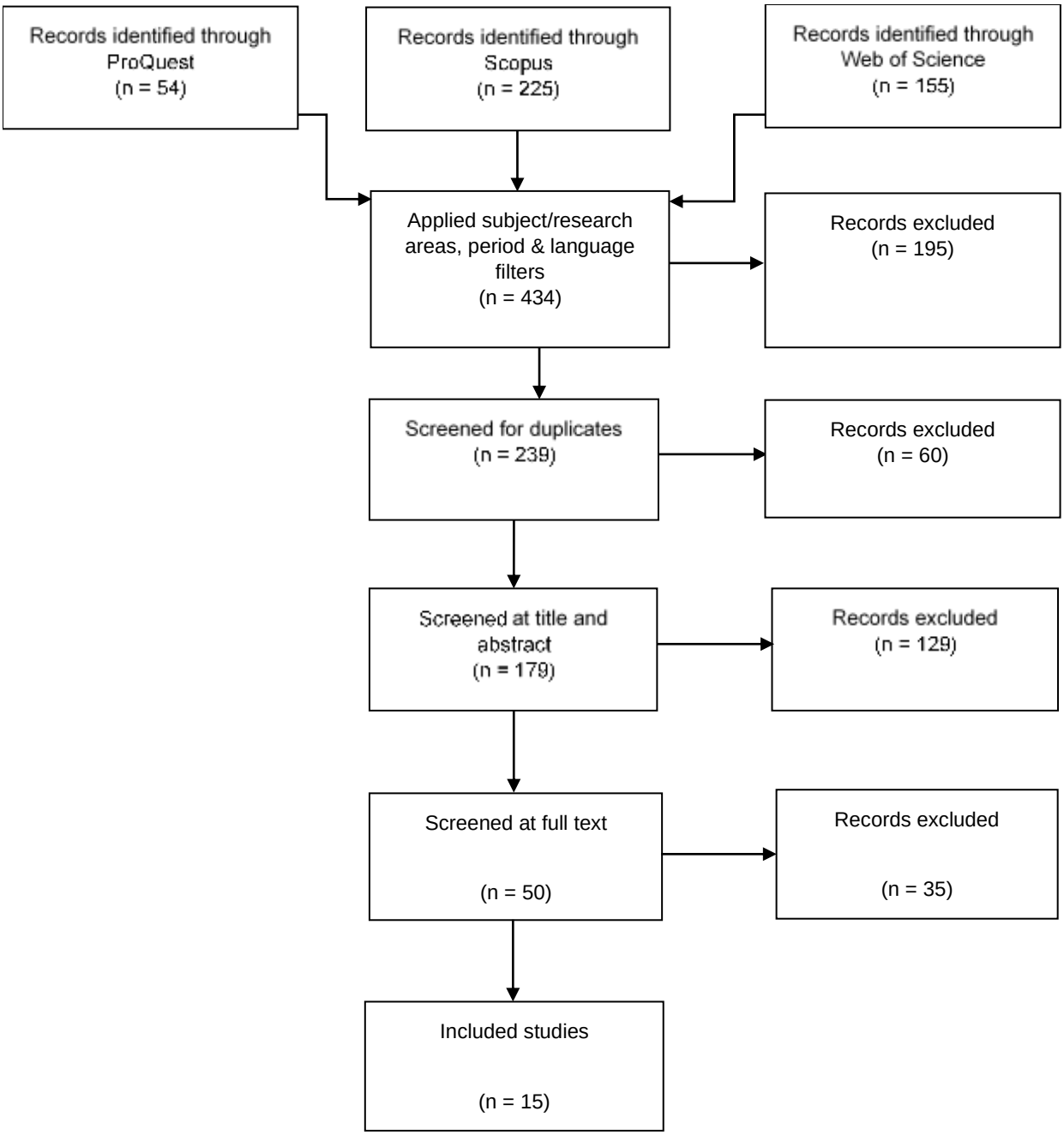
Systematic review results

A total of 434 results were returned across the three databases which were eventually screened to the 15 studies selected for this assessment. Figure 1 summarises the screening and inclusion process employed to choose the final studies. Selected studies were all primary and significantly qualitative with the exception of two studies which adopted a mixed methods approach[21,22]. Using the evidence appraisal scheme described in Table 2, these studies were prioritised in descending order of validity. This prioritisation was required to ensure only studies that directly addressed the research questions in the context of safeguarding online privacy against information leakages were reviewed. For instance, one paper which assessed personal responsibility and online privacy was excluded because it reflected the context of cultural norms expected of a particular group in India regarding SNSs use[23].

Table 2 *Appraisal Scheme for assessing evidence*

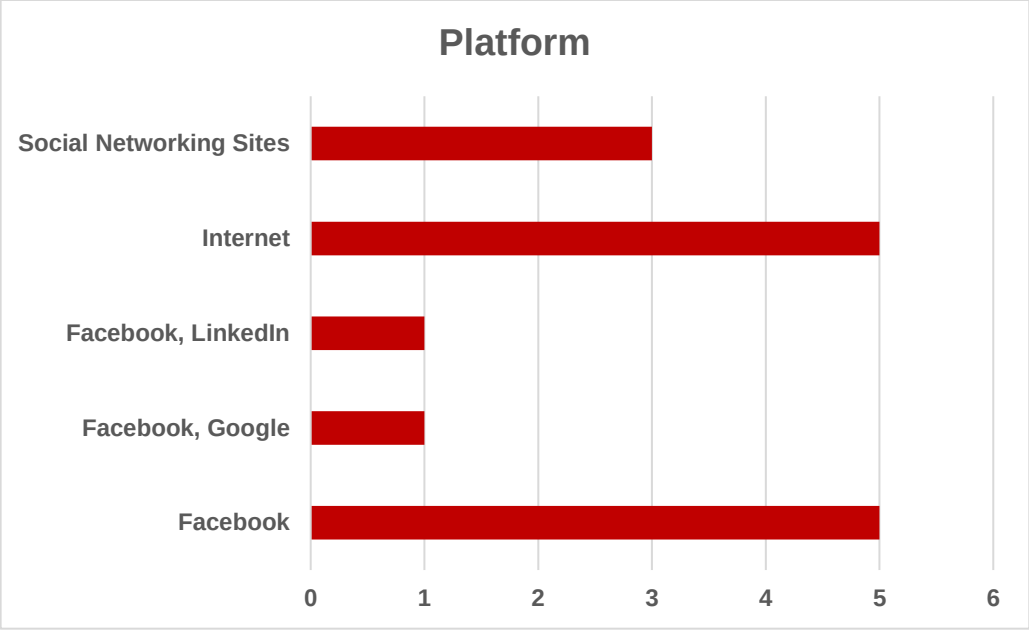
Evidence Type	Description
Experimental	Involves evaluating hypotheses on randomly assigned user groups. Participants were also required to execute a series of instructions to test the hypotheses.
Simulation/model	Involves testing hypotheses on a model using qualitative data
Thematic/textual analysis	Involves coding themes identified and obtained from qualitative data

Figure 1 *PRISMA chart showing systematic search process results*



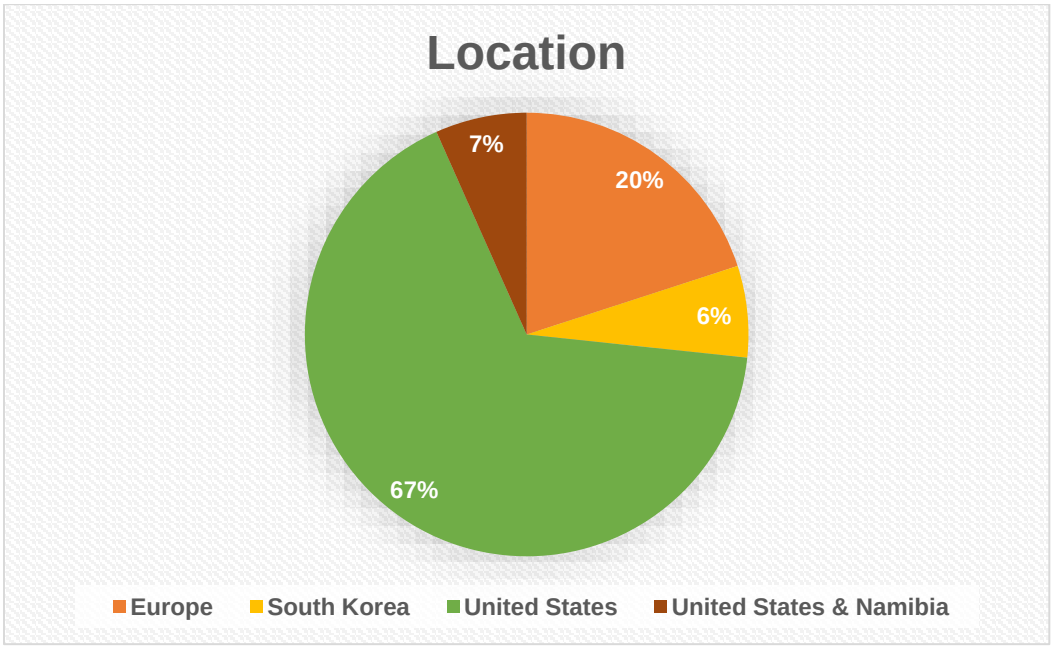
As illustrated in Figure 2, Facebook is the platform most observed for user activity across the 15 studies. Studies that analysed multiple platforms (e.g. Facebook & LinkedIn) are indicated in their individual categories in order not to distort the distribution or misrepresent the findings. In addition, the SNSs component comprises studies that did not explicitly specify or focus on any SNS, while Internet represents user activity such as online shopping and could also imply use of SNSs in general[24,25].

Figure 2 *Included studies by platform category*



Although this REA was not confined to a specific location, a geographic distribution of the scoped studies is presented in Figure 3. This visual[1] is helpful as it indicates a possible representation gap in the studies that have been conducted thus far.

Figure 3 *Included studies by geographic location*



[1] One study outlines a comparison between college students in the United States and Namibia[21], while three studies collectively make up the Europe segment comprising eight countries [26–28].

Findings

The findings from the 15 studies are analysed in three sub-sections highlighting similar themes observed during the REA. A summary of the included studies is here presented in Table 3.

Table 3 *Included studies mapped to sub-research questions (SRQ)*

S/n	Title	Author(s)	Evidence Type	SRQ 1	SRQ 2	SRQ 3
1	Determinants of online safety behaviour: Towards an intervention strategy for college students	Boehmer J., LaRose R., Rifon N., Alhabash S., Cotten S.	Experimental	X		X
2	Online safety begins with you and me: Convincing Internet users to protect themselves	Shillair R., Cotten S.R., Tsai H.-Y.S., Alhabash S., Larose R., Rifon N.J.	Experimental	X		X
3	Cultural and generational influences on privacy concerns: a qualitative study in seven European countries	Miltgen, CL; Peyrat-Guillard, D	Simulation/model	X	X	
4	Making privacy personal: Profiling social network users to inform privacy education and nudging	Wisniewski, PJ; Knijnenburg, BP; Lipford, HR	Simulation/model		X	X
5	Regrets, I've had a few: When regretful experiences do (and don't) compel users to leave Facebook	Guha S., Baumer E.P.S., Gay G.K.	Simulation/model		X	X
6	Factors predicting attitude toward disclosing personal data online	Robinson S.C.	Simulation/model	X		
7	Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook: An empirical investigation	Taneja A., Vitrano J., Gengo N.J.	Simulation/model	X	X	X
8	Self-censorship in social networking sites (SNSs) – privacy concerns, privacy awareness, perceived vulnerability and information management	Warner M., Wang V.	Simulation/model	X	X	
9	Self-concepts in cyber censorship awareness and privacy risk perceptions: What do cyber asylum-seekers have?	Jin C.-H.	Simulation/model		X	
10	The post that wasn't: Exploring self-censorship on facebook	Sleeper M., Balebako R., Das S., McConahy A.L., Wiese J., Cranor L.F.	Thematic/textual analysis		X	
11	“Nobody sees it, nobody gets mad”: Social media, privacy, and personal responsibility among low-SES youth	Marwick A., Fontaine C., Boyd D.	Thematic/textual analysis	X	X	
12	“It's not like they're selling your data to dangerous people”: Internet privacy, teens, and (non-)controversial public issues	Crocco M.S., Segall A., Halvorsen A.-L., Stamm A., Jacobsen R.	Thematic/textual analysis	X		
13	Cultural influences on Facebook practices: A comparative study of college students in Namibia and the United States	Peters A.N., Winschiers-Theophilus H., Mennecke B.E.	Thematic/textual analysis	X	X	
14	From Youthful Experimentation to Professional Identity: Understanding Identity Transitions in Social Media	Brandtzaeg P.B., Chaparro-Domínguez M.-Á.	Thematic/textual analysis		X	
15	Organizations' Responsibility in Maintaining The Security Of Personal Data Posted Online By Romanian Consumers: An Exploratory Analysis Of Facebook And LinkedIn	Ionescu, Andreea;Anghel, Laurentiu-Dan;Jinga, Gheorghe	Thematic/textual analysis		X	

Personal Responsibility and Safeguarding Privacy Online

A cross-section of the findings suggests that not only should users be responsible for preserving their privacy on digital platforms, they are expected to educate themselves as well[25,26,29–31]. Feedback from respondents analysed by the authors imply the reasons for personal responsibility range from users being: aware of the privacy risks involved[26], accountable for managing (the spread of) their information[25,30,31] and in need of services from an online provider[29].

Several of the studies[21,26,29,32] also appear to indicate that the relationship between citizens and the state or government impacts on users being personally responsible for safeguarding their privacy in online environments. Collectivist societies which tend to trust the state relinquish responsibility for their privacy to it, whereas individualistic cultures acknowledge that individuals are responsible for protecting their privacy online[26]. Thus, citizens in collectivist countries are more likely to exhibit behaviours like self-disclosing information or using privacy settings to prevent contacts on their friends' lists from viewing certain posts but not to exclude information they believe to be common knowledge[21]. Findings also indicate geographical location has no effect on these behaviours; for instance, while it is noted that the United States is largely individualistic, European countries consisting of both collectivist and individualistic countries displayed traits noted for each respective group.

Despite the apparent influence of national cultures on citizens' privacy behaviours, two studies from the United States[29,30] suggest that framing privacy protection as individualistic is too narrow a lens to sufficiently tackle privacy-related concerns. Drawing parallels with indiscriminate policing over which low-income youth in New York have little control, Marwick et al highlight that the inherent power imbalance between citizens and corporations would hamper individuals' ability to adequately preserve their privacy without external measures[30]. Likewise, some studies recommend that individuals may be encouraged to embrace personal responsibility for their privacy by observing how more privacy-aware persons navigate online environments or through targeted messages that cater to unique user abilities [24,33].

Factors enabling Proactive Privacy Protection

Some studies[27,30,34,35] indicate that the concept of "networked privacy" whereby relationships are forged through SNSs, could be a deciding factor to proactively protect privacy, as the actions of one individual could impact the privacy of their connections or network. In this way, individuals adopt self-censoring habits by choosing to limit personal information on digital platforms or electing to not post anything at all.

In addition, some authors identify trust as an underlying factor in users being deliberate about preserving their privacy online. Where trust in governments or corporations (i.e. technology companies) is low, analysis of survey data suggests that users' awareness of privacy concerns is heightened which leads to increased self-censorship on online environments[22,25,26,32]. Furthermore, the Jin paper describes how individuals who "are more familiar with technology" and have increased self-respect are more aware of cyber-censorships by state or private actors, and are therefore likely to be more proactive in securing their privacy online[36]. Still regarding trust, Ionescu et al posit that by implementing the ISO 26000 standard which provides guidance to social responsibility, organisations may be able to help users adopt safer online practices[28].

A selection of the studies indicates knowledge of privacy control features available on SNSs as being influential in nudging individuals to observe safe online behaviours[31,34]. However, the findings also highlight that individuals' use of these features is dependent on their usability. Accordingly, if these features were deemed not user-friendly, users indicated a likelihood that they would not exploit them, thus resulting in insecure online practices[22].

Individuals were noted to also modify their posting habits on the Internet and SNSs when they sought to selectively present themselves in a desired light to certain audiences like parents, employers or acquaintances[21,22]. In adopting such habits, individuals seem to exercise an intention to manage their online information in a safe way. A study of young journalists in Norway and Spain also found that their profession directly impacted their activities online as they sought to distance themselves from their adolescent "digital selves" by selectively curating their present digital selves[27].

Effectiveness of Factors in influencing Proactive Privacy Protection Online

Employing experimental methods and simulations to test designed hypotheses, several studies[24,31,33–35] attempt to show how strategies to protect privacy online may be effectively adopted. Two studies extend the Protection Motivation Theory (PMT) model which was developed to explain how individuals may be motivated to react protectively against perceived threats to them[37] and has been used in fields including health and psychology. Incorporating "personal responsibility" as an additional variable in the PMT model, Boehmer et al conducted an experiment by presenting opposing messages on responsibility for online privacy to two groups comprising US college students[24]. Findings indicate that while it is possible to induce individuals to be responsible for preserving their privacy online, this strategy may not be effective for novice Internet users. Similarly, the experiment by Shillair et al randomly assigned users to four separate groups and fed them with individual messages on personal responsibility. However, this experiment found that combining messaging with graphical procedures for navigating online platforms safely was more effective than merely offering instructions or tips to both experienced and novice users[33].

Some studies have found that privacy controls may need to be redesigned to enable users more actively manage their personal information and privacy online. Considering the interconnectedness of SNSs, findings indicate that redesigned privacy configurations could also provide for networked privacy such that posting actions of an individual do not negatively impact his/her connections[34,35]. Additionally, it has been noted that certain attitudes such as seeing privacy controls as being beneficial influenced users to seek out and use them[31]. This study[31] also finds that individuals engage privacy controls if they are convinced that the controls can help to limit access to their information. Finally, by knowing individuals' privacy management behaviours, personalised nudging strategies for safer online navigation can be developed. Without this knowledge however, it would not be possible to craft such strategies. One point to note overall is that studies suggesting a redesign of privacy controls are limited to Facebook.

Conclusions

In view of recent privacy breaches on the Internet and SNSs, this REA set out to investigate the role of personal responsibility in enabling individuals to preserve their privacy on these platforms. Existing evidence indicates that online privacy protection is an ongoing discussion among researchers seeking practical strategies which users can adopt. While the body of evidence presented in this REA highlights these strategies to include privacy control redesign and personalised education/awareness, these interventions are largely restricted to Facebook. Thus, there may be a need to research other SNSs to verify the applicability of such strategies. In addition, some of the research conducted on privacy behaviours relied on self-reported data from survey respondents which may not be without bias[22,32,34,35]. Hence, future research may need to consider ways to test these behaviours in a more realistic or objective setting.

Another consideration regarding future research would be to extend proposed strategies for enabling personal responsibility, like the modified PMT model and privacy behaviours, to more

demographic groups since the reviewed studies focused solely on young college students. This is because users of the Internet and SNSs span across diverse categories.

As two-thirds of the research papers originate from the United States, this raises the question of the validity of the findings in other regions of the world, particularly Africa and South Asia where Internet penetration hovers around 19%[38]. Given that the Internet growth rate is projected to close this gap by 2023[2], research focused on developing strategies salient to these regions is required to address their privacy management needs.

References

1. Annual Report 2019-2020 - Key Stats: First results of the new ITU Strategic Plan 2020-23 [Internet]. [cited 2021 Feb 20]. Available from: https://itu.foleon.com/itu/annual-report-2019-2020/key-stats-first-results-of-the-new-itu-strategic-plan-2020-23/

2. Connect 2030 Agenda - Home [Internet]. [cited 2021 Apr 3]. Available from: https://itu.foleon.com/itu/connect-2030-agenda/home/

3. Number of social media users 2025 [Internet]. Statista. [cited 2021 Feb 20]. Available from: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

4. Mastering the challenge of balancing self-disclosure and privacy in social media | Elsevier Enhanced Reader [Internet]. [cited 2021 Feb 20]. Available from: https://reader.elsevier.com/reader/sd/pii/S2352250X19301265?token=C66EC21C54A682B923AE9880AAB525C26731EF9E53AB3D0EA90670F2E709F3A0C3453CD7126E8EBA0DDAB6D3D65B8003 https://doi.org/10.1016/j.copsyc.2019.08.003.

5. Exploring users' motivations to participate in viral communication on social media | Elsevier Enhanced Reader [Internet]. [cited 2021 Feb 20]. Available from: https://reader.elsevier.com/reader/sd/pii/S0148296318305630?token=0CC54473F7FA795C8FB8B4AF6532B42CB39B7401E937E03B84FDCB4B7DF90209C81CF75880FA8A6755481C270ECC63D2 https://doi.org/10.1016/j.jbusres.2018.11.011.

6. Deibert RJ. Three Painful Truths About Social Media. *J Democr* 2019;**30**:25–39. https://doi.org/10.1353/jod.2019.0002.

7. 1195716.pdf [Internet]. [cited 2021 Apr 1]. Available from: https://dl.acm.org/doi/pdf/10.1145/1195716.1195721

8. Zittrain JL. THE GENERATIVE INTERNET. *Harv LAW Rev* :67.

9. Carr CT, Hayes RA. Social Media: Defining, Developing, and Divining. *Atl J Commun* 2015;**23**:46–65. https://doi.org/10.1080/15456870.2015.972282.

10. Kekulluoglu D, Kokciyan N, Yolum P. Preserving Privacy as Social Responsibility in Online Social Networks. *ACM Trans Internet Technol* 2018;**18**:1–22. https://doi.org/10.1145/3158373.

11. Reid GG, Boyer W. Social Network Sites and Young Adolescent Identity Development. *Child Educ* 2013;**89**:243–53. https://doi.org/10.1080/00094056.2013.815554.

12. Joo T-M, Teng C-E. Impacts of Social Media (Facebook) on Human Communication and Relationships: A View on Behavioral Change and Social Unity. *Int J Knowl Content Dev Technol* 2017;**7**:27–50. https://doi.org/10.5865/IJKCT.2017.7.4.027.

13. Kelly M. MyHeritage breach leaks millions of account details [Internet]. The Verge. 2018 [cited 2021 Apr 2]. Available from: https://www.theverge.com/2018/6/5/17430146/dna-myheritage-ancestry-accounts-compromised-hack-breach

14. The Infamous Ashley Madison Hack: What Exactly Happened? [Internet]. The Dark Web Journal. 2020 [cited 2021 Apr 2]. Available from: https://darkwebjournal.com/ashley-madison-hack/

15. Temperton J. The Ashley Madison data breach is already ruining lives. *Wired UK* 2015 Aug 19 [cited 2021 Apr 2]; Available from: https://www.wired.co.uk/article/ashley-madison-have-i-been-hacked

16. Waterfield TR and P. Huge new Facebook data leak exposed intimate details of 3m users [Internet]. New Scientist. [cited 2021 Apr 2]. Available from: https://www.newscientist.com/article/2168713-huge-new-facebook-data-leak-exposed-intimate-details-of-3m-users/

17. Facebook breach shows “we share too much and think too little” [Internet]. [cited 2021 Apr 2]. Available from: https://www.cbsnews.com/news/facebook-breach-shows-we-share-too-much-and-think-too-little/

18. Barnes R, Potter A. Sharenting and parents’ digital literacy: an agenda for future research. *Commun Res Pract* 2020:1–15. https://doi.org/10.1080/22041451.2020.1847819.

19. Park YJ. Digital Literacy and Privacy Behavior Online. *Commun Res* 2013;**40**:215–36. https://doi.org/10.1177/0093650211418338.

20. Boddy J, Dominelli L. Social Media and Social Work: The Challenges of a New Ethical Space. *Aust Soc Work* 2017;**70**:172–84. https://doi.org/10.1080/0312407X.2016.1224907.

21. Cultural influences on Facebook practices: A comparative study of college students in Namibia and the United States | Elsevier Enhanced Reader [Internet]. [cited 2021 Apr 5]. Available from: https://reader.elsevier.com/reader/sd/pii/S0747563215001892?token=9612217C27364045545EA615B8A142A3CF8665108FDCFEA089007E2BAA3AC46C982EA56D5C2C28590740BF733719E046&originRegion=eu-west-1&originCreation=20210405132903 https://doi.org/10.1016/j.chb.2015.02.065.

22. Sleeper M, Balebako R, Das S, McConahy AL, Wiese J, Cranor LF. The post that wasn’t: exploring self-censorship on facebook. In: *Proc 2013 Conf Comput Support Coop Work - CSCW 13* San Antonio, Texas, USA: ACM Press, 2013 [cited 2021 Apr 5].p.793. Available from: http://dl.acm.org/citation.cfm?doid=2441776.2441865 https://doi.org/10.1145/2441776.2441865.

23. Mishra S, Basu S. Family honor, cultural norms and social networking: Strategic choices in the visual self-presentation of young Indian Muslim women. *Cyberpsychology J Psychosoc Res Cyberspace* 2014;**8**. https://doi.org/10.5817/CP2014-2-3.

24. Boehmer J, LaRose R, Rifon N, Alhabash S, Cotten S. Determinants of online safety behaviour: towards an intervention strategy for college students. *Behav Inf Technol* 2015;**34**:1022–35. https://doi.org/10.1080/0144929X.2015.1028448.

25. Robinson SC. Factors predicting attitude toward disclosing personal data online. *J Organ Comput Electron Commer* 2018;**28**:214–33. https://doi.org/10.1080/10919392.2018.1482601.

26. Miltgen CL, Peyrat-Guillard D. Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *Eur J Inf Syst* 2014;**23**:103–25. https://doi.org/10.1057/ejis.2013.17.

27. Brandtzaeg PB, Chaparro-Domínguez M-Á. From Youthful Experimentation to Professional Identity: Understanding Identity Transitions in Social Media. *YOUNG* 2020;**28**:157–74. https://doi.org/10.1177/1103308819834386.

28. Ionescu A, Anghel L-D, Jinga G. Organizations’ Responsibility in Maintaining the Security of Personal Data Posted Online by Romanian Consumers: An Exploratory Analysis of Facebook and Linkedin. *Amfiteatru Econ* 2014;**16**:273–88.

29. ``It’s not like they’re selling your data to dangerous people’’: Internet privacy, teens, and (non-)controversial public issues | Elsevier Enhanced Reader [Internet]. [cited 2021 Apr 5]. Available from: https://reader.elsevier.com/reader/sd/pii/S0885985X1930172X?token=B61AE35268AF4FA60D93A8C817DE94249E12D7B4FE729218982072A0EC261F35E730C2CCE9D1EF7EDB6ACD39E417D37

D&originRegion=eu-west-1&originCreation=20210405131422 https://doi.org/10.1016/j.jssr.2019.09.004.

30. Marwick A, Fontaine C, boyd danah. “Nobody Sees It, Nobody Gets Mad”: Social Media, Privacy, and Personal Responsibility Among Low-SES Youth. *Soc Media Soc* 2017;**3**:2056305117710455. https://doi.org/10.1177/2056305117710455.

31. Rationality-based beliefs affecting individualâ€™s attitude and intention to use privacy controls on Facebook: An empirical investigation | Elsevier Enhanced Reader [Internet]. [cited 2021 Apr 5]. Available from: https://reader.elsevier.com/reader/sd/pii/S0747563214003057?token=07BB337014EC317139393C73C6A653834B650B1C5B1BFF0E493B5EE1477FBD2F9830B077860AADD9285B258C3597ECCD&originRegion=eu-west-1&originCreation=20210405133635 https://doi.org/10.1016/j.chb.2014.05.027.

32. Warner M, Wang V. Self-censorship in social networking sites (SNSs) – privacy concerns, privacy awareness, perceived vulnerability and information management. *J Inf Commun Ethics Soc* 2019;**17**:375–94. https://doi.org/10.1108/JICES-07-2018-0060.

33. Online safety begins with you and me: Convincing Internet users to protect themselves | Elsevier Enhanced Reader [Internet]. [cited 2021 Apr 5]. Available from: https://reader.elsevier.com/reader/sd/pii/S0747563215000606?token=4BAD09C0C55BE5F8C10CEDC773A200488D0699F95687C1A8B246A3DC03EAD3EBE1B656E59B83FE1D0AFE3A986A11FEC5&originRegion=eu-west-1&originCreation=20210405133514 https://doi.org/10.1016/j.chb.2015.01.046.

34. Making privacy personal_ Profiling social network users to inform privacy education and nudging | Elsevier Enhanced Reader [Internet]. [cited 2021 Apr 5]. Available from: https://reader.elsevier.com/reader/sd/pii/S1071581916301185?token=83DED26DD7EAEF1A7A3741A90D9AD324188C71B002C03967D6D9908081215BA0A7D242E687E57D30DAFA60A8CFCAD02F&originRegion=eu-west-1&originCreation=20210405131734 https://doi.org/10.1016/j.ijhcs.2016.09.006.

35. Guha S, Baumer EPS, Gay GK. Regrets, I’ve Had a Few: When Regretful Experiences Do (and Don’t) Compel Users to Leave Facebook. In: *Proc 2018 ACM Conf Support Groupwork* Sanibel Island Florida USA: ACM, 2018 [cited 2021 Apr 5].p.166–77. Available from: https://dl.acm.org/doi/10.1145/3148330.3148338 https://doi.org/10.1145/3148330.3148338.

36. Self-concepts in cyber censorship awareness and privacy risk perceptions: What do cyber asylum-seekers have? | Elsevier Enhanced Reader [Internet]. [cited 2021 Apr 5]. Available from: https://reader.elsevier.com/reader/sd/pii/S0747563217306660?token=6B6657CA68202D147FE689CB617C58B0858093599753FD82B0E8C69F9626D57A41920CFB878C86AE4CB20DDB4A270143&originRegion=eu-west-1&originCreation=20210405133724 https://doi.org/10.1016/j.chb.2017.11.028.

37. Westcott R, Ronan K, Bambrick H, Taylor M. Expanding protection motivation theory: investigating an application to animal owners and emergency responders in bushfire emergencies. *BMC Psychol* 2017;**5**:13. https://doi.org/10.1186/s40359-017-0182-3.

38. FactsFigures2019.pdf [Internet]. [cited 2021 Apr 11]. Available from: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

39. Global regional internet penetration rate 2021 [Internet]. Statista. [cited 2021 Feb 20]. Available from: https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/

40. Connect 2030 Agenda - Home [Internet]. [cited 2021 Feb 20]. Available from: https://itu.foleon.com/itu/connect-2030-agenda/home/

41. The rise of social media [Internet]. Our World in Data. [cited 2021 Feb 20]. Available from: https://ourworldindata.org/rise-of-social-media

Annex 1: REA Protocol

Title	Investigating the role of personal responsibility in safeguarding privacy in online engagements
Summary	The global Internet penetration rate has steadily risen since 2005[1] and is presently at 59.5%[39]. According to the International Telecommunication Union, this rate is predicted to increase to 70% by 2023[40]. Social media is also projected to be used by over 4 billion people globally by 2025[3]. Trends like participatory social media challenges intensify the propensity of its users to self-disclose or share personal information[4,5], sometimes inadvertently, on these platforms. Congruent with these advancements is the increase in privacy-related breaches such as the harvesting of user data by Cambridge Analytica to allegedly influence voter sentiment in the 2016 Brexit referendum and United States presidential elections[6]. There is a need to investigate user awareness of online privacy and factors that influence individuals to protect their privacy while engaging on social media and the Internet in general. Consequently, this systematic review aims to identify existing research on the role of personal responsibility in safeguarding privacy on digital platforms including social networking sites and the Internet. It is expected that the review findings would contribute to the ongoing data privacy discourse and strengthen the argument for improving user awareness in using these platforms. Additionally, insights surfaced from the review may present the opportunity to explore further research topics in the data privacy domain.
Research question **Sub-questions**	What evidence exists to show that personal responsibility plays a role in users safeguarding their privacy in online environments (digital platforms including the Internet and social networking sites)? • To what extent does personal responsibility influence user behaviour in protecting privacy on digital platforms? • What factors aid users in proactively protecting their privacy on digital platforms? • How effective are these factors in influencing users to be responsible for their privacy on digital platforms?
Academic Databases	• ProQuest Central: provides access to 50 databases of research material covering subject areas like multidisciplinary studies, science and technology studies and the social sciences. • Scopus: this interdisciplinary database comprises titles from social sciences, physical sciences, health sciences, and life sciences subject areas. • Web of Science Core Collection: provides focused access to scholarly material across a wide range of subject areas including social sciences, sciences, and the humanities. Source materials include books, journals, and proceedings. In addition, all databases provide functionalities to filter for date, subject area, publication type, and source type.
Disciplines	Though captured with different nomenclature across the selected databases, the scoped disciplines are broadly similar as indicated below: **ProQuest Subjects:** Due to the granular level of subjects in the ProQuest database, these details (42) are in Appendix C. **Scopus Subject Areas:** Computer Science, Engineering, Social Sciences, Arts & Humanities, Economics, Econometrics and Finance, Psychology, Decision Sciences and Multidisciplinary

	Web of Science Research Areas: Computer Science, Engineering, Social Sciences, Psychology, Science Technology, Social Issues, Sociology and Neurosciences
Inclusion and exclusion	The review will include studies: • using a range of methodologies including qualitative, quantitative, mixed methods, case studies, and other evidence reviews. • indicating user interactions with digital platforms including social media and the Internet in general. • discussing user behaviours and attitudes to privacy on digital platforms. The review will exclude: • all studies that are not peer-reviewed. • all publications that are not at the final stage. • all publications not available in English due to the researcher's primary language skills being English and limited resources available for the review. • Medical Science related papers as their focus appears to be on medical ethics like secure management/disclosure of patient information, which does not fully address the research question(s). • Business, Management and Accounting related studies because they address privacy concerns through the lenses of firms and markets and not the individual.
Search strategy	The review will employ the following terms derived from the research question to search selected databases (cited below is the syntax for ProQuest). Detailed queries for all databases are listed in Appendix B of this document. • ((user NEAR/3 responsibility) OR (consumer NEAR/3 responsibility) OR (citizen NEAR/3 responsibility) OR (personal NEAR/3 responsibility) OR (individual NEAR/3 responsibility) OR (user NEAR/3 accountability) OR (consumer NEAR/3 accountability) OR (citizen NEAR/3 accountability) OR (personal NEAR/3 accountability) OR (individual NEAR/3 accountability) OR (user NEAR/3 agenc*) OR (consumer NEAR/3 agenc*) OR (citizen NEAR/3 agenc*) OR (personal NEAR/3 agenc*) OR (individual NEAR/3 agenc*) OR ("self-censor*") OR ("self censor*") OR (self NEAR/3 censor*))) **AND** • (privacy OR secur* OR safe* OR protect* OR private) **AND** • ((social NEAR/3 media) OR ("online social network*") OR (social NEAR/3 networking NEAR/3 site*) OR ("online platform*") OR ("digital platform*") OR (internet) OR (cyber)) OR ab((social NEAR/3 media) OR ("online social network*") OR (social NEAR/3 networking NEAR/3 site*) OR ("online platform*") OR ("digital platform*") OR (internet) OR (cyber)) **AND** • (meta-analy* OR "systematic review" OR design or study or analysis OR intervention* OR "quasi experiment*" or quasi-experiment* OR experiment*)

	Searches will be limited to the period from 2010 till date i.e. 2021. 2010 was selected as the anchor year because social media users surpassed the 1 billion mark for the first time ever that year[41]. The period was chosen to retrieve the most recent research available and to manage the scale of searches returned.
Literature management	Search results will be imported and maintained in individual folders created for each database source on the Zotero reference manager application, to aid referencing and future retrieval.
Selection of studies	The initial search will be conducted at the abstract, title and keywords levels in each database. Search results would then be filtered using in-scope subject areas and analysed for duplicate records, which will be excluded. The final screened studies will be obtained by: • reviewing abstracts for relevance to inclusion criteria and research questions • conducting full-text reviews of studies that satisfy the inclusion criteria • extracting and sorting studies based on how they address each sub-question
Strategy for data synthesis	To enable an efficient synthesis, the final screened studies will be categorised along two dimensions; a coding framework to highlight how relevant each study is to the research question and an evidence appraisal scheme, which are further explained in the Included Studies and Preliminary Results section below.

Included Studies and Preliminary Results

Database searches and Filtering

The database searches were conducted between February and March 2021 across three electronic databases; ProQuest, Scopus and Web of Science. Search queries were developed from concepts (personal responsibility, privacy and online) derived from the main research question and some elements of the sub-questions. The detailed concepts table is included in Appendix A.

To ensure a relatively high relevance of results was returned, queries were individually built for each concept and then combined to arrive at a final search query. Afterwards, the search query was applied in the databases, with the only difference being variations in the syntax recognised by each database. The searches were conducted at the abstract, title and keywords levels, using the terms detailed in the Search Strategy section above. Searches were limited to papers published from 2010 till date, restricted to peer-reviewed studies and filtered for English results only, as also stated in the previous section.

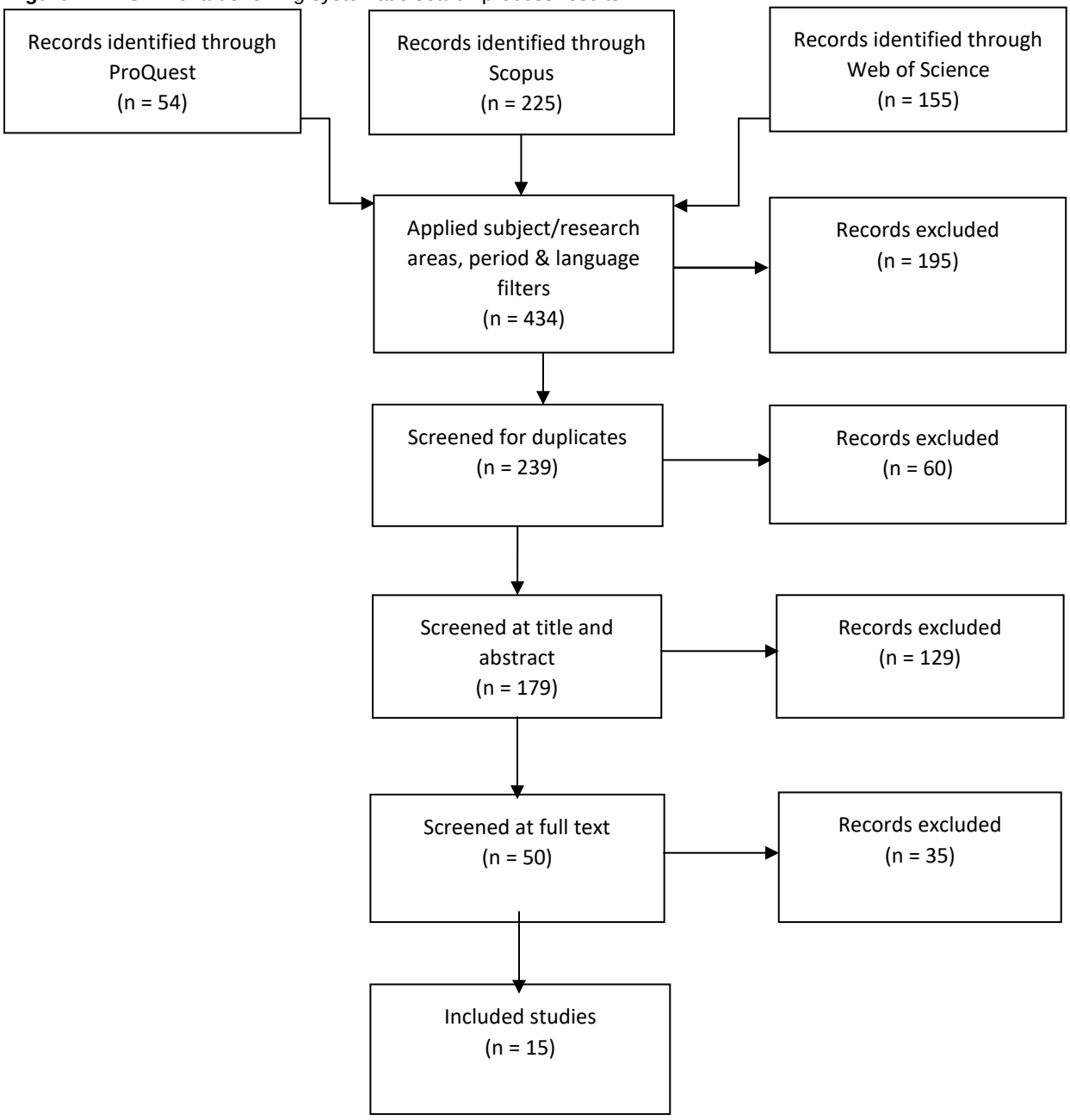
No document type was excluded from the search, i.e. results comprised journal articles, book chapters, conference papers etc. The initial search results amounted to 434 (ProQuest – 54, Scopus – 225 and Web of Science – 155). Subject area, period and language filters were then applied in each database which led to an exclusion of 195 studies from the initial findings to yield a total of 239 studies. These results were individually exported from each database into Research Information Systems (RIS) and text file formats. Next, the files were imported into the Zotero reference management software. In addition, the files were exported in Comma Separated Values and Microsoft Excel file formats from which the following similar fields were extracted and then combined to form a new data set in Microsoft Excel:

- Database
- Author
- Article Title
- Article Type
- Source Title
- Digital Object Identifier (DOI)
- Year
- Abstract

Due to differences in some of the exported file formats, running a full duplicates check on all the records using Zotero was not entirely feasible. Instead, the duplicates check was conducted on the combined data set using Microsoft Excel. 60 duplicate records were detected and excluded from the data set leaving 179 studies which would be screened at full-text for the systematic review.

The process described above to select the 179 eligible studies for additional screening during the systematic review phase is summarised in the adapted PRISMA flowchart below:

Figure 1 PRISMA chart showing systematic search process results

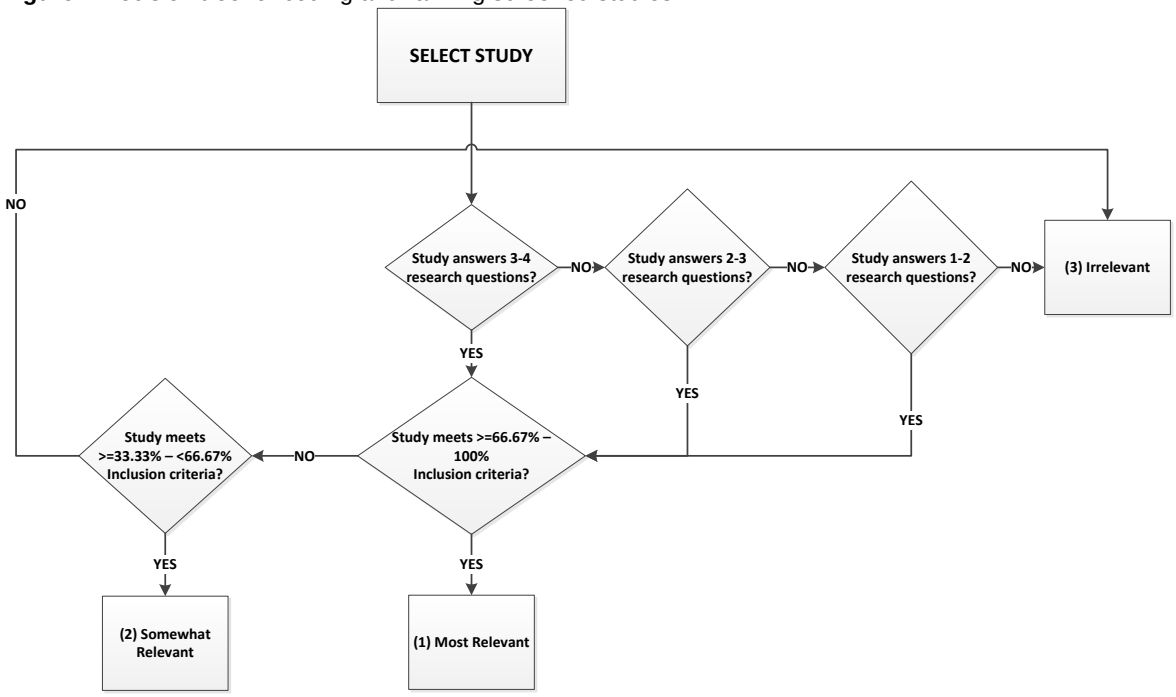


Data Extraction and Synthesis Strategy

This process proceeded with reading each title and abstract of the 179 results to determine if they aligned with the inclusion criteria, as well as to identify any of the search terms or concepts. Studies with abstracts that fully or partially met these criteria shall be read in full while those that did not satisfy any of the criteria were excluded from further review. The justification for including partly compliant studies is to capture enough data and to prevent unintentional omissions that may be relevant to the systematic review. Following this abstract screening, 129 studies were excluded because they did not directly address the main research and sub-research questions. Topics covered in the excluded studies ranged from e-government, social media use in government and companies, cloud technology and ethical use of social media.

Two dimensions were constructed to aid classification and efficient synthesis of the remaining 50 studies; a coding framework and an evidence appraisal scheme. These tools are also aimed at prioritising the studies at the synthesis stage. Devised from a combination of the inclusion criteria and research question (sub-questions inclusive), the coding framework will be applied to rank the studies in order of relevance. The framework is intended to indicate the extent of individuals' awareness of their privacy while engaging in Internet-mediated activities, including social media. Studies reflecting up to 100% alignment with the coding framework as depicted in Figure 2 will be prioritised as "most relevant" representing the highest degree of salience. Conversely, studies that satisfy less than 33.33% of the framework requirements will be classified as "irrelevant".

Figure 2 Decision tree for coding and ranking screened studies



The evidence appraisal scheme was used to assess and categorise the various methodologies adopted in each study to determine their validity i.e. how representative they are of the policy problem. Studies will be broadly classified as either quantitative, qualitative, mixed-methods and evidence reviews as applicable, and would be further decomposed into sub-categories based on findings from the full-text reading. These sub-categories form the evidence appraisal scheme which is outlined in Table 1 below; experimental studies represent the highest validity while thematic studies are ranked as having the least validity. With

the likelihood of diverse methodologies being represented, a narrative approach will be used to synthesise the final screened studies.

Table 1 Appraisal Scheme for assessing evidence

Evidence Type	Description
Experimental	Involves evaluating hypotheses on randomly assigned user groups. Participants were also required to execute a series of instructions to test the hypotheses.
Simulation/model	Involves testing hypotheses on a model using qualitative data
Thematic/textual analysis	Involves coding themes identified and obtained from qualitative data

REFERENCE LIST

1. Annual Report 2019-2020 - Key Stats: First results of the new ITU Strategic Plan 2020-23 [Internet]. [cited 2021 Feb 20]. Available from: https://itu.foleon.com/itu/annual-report-2019-2020/key-stats-first-results-of-the-new-itu-strategic-plan-2020-23/

2. Global regional internet penetration rate 2021 [Internet]. Statista. [cited 2021 Feb 20]. Available from: https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region/

3. Connect 2030 Agenda - Home [Internet]. [cited 2021 Feb 20]. Available from: https://itu.foleon.com/itu/connect-2030-agenda/home/

4. Number of social media users 2025 [Internet]. Statista. [cited 2021 Feb 20]. Available from: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

5. Mastering the challenge of balancing self-disclosure and privacy in social media | Elsevier Enhanced Reader [Internet]. [cited 2021 Feb 20]. Available from: https://reader.elsevier.com/reader/sd/pii/S2352250X19301265?token=C66EC21C54A682B923AE9880AAB525C26731EF9E53AB3D0EA90670F2E709F3A0C3453CD7126E8EBA0DDAB6D3D65B8003 https://doi.org/10.1016/j.copsyc.2019.08.003.

6. Exploring users' motivations to participate in viral communication on social media | Elsevier Enhanced Reader [Internet]. [cited 2021 Feb 20]. Available from: https://reader.elsevier.com/reader/sd/pii/S0148296318305630?token=0CC54473F7FA795C8FB8B4AF6532B42CB39B7401E937E03B84FDCB4B7DF90209C81CF75880FA8A6755481C270ECC63D2 https://doi.org/10.1016/j.jbusres.2018.11.011.

7. Deibert RJ. Three Painful Truths About Social Media. *J Democr* 2019;**30**:25–39. https://doi.org/10.1353/jod.2019.0002.

8. The rise of social media [Internet]. Our World in Data. [cited 2021 Feb 20]. Available from: https://ourworldindata.org/rise-of-social-media

APPENDIX A: RESEARCH CONCEPTS

Concept 1: Online	**Concept 2:** Personal Responsibility	**Concept 3:** Privacy	**Concept 4:** Evidence
(social NEAR/3 media) OR ("online social network*") OR (social NEAR/3 networking NEAR/3 site*) OR ("online platform*") OR ("digital platform*") OR (internet) OR (cyber)	(user NEAR/3 responsibility) OR (consumer NEAR/3 responsibility) OR (citizen NEAR/3 responsibility) OR (personal NEAR/3 responsibility) OR (individual NEAR/3 responsibility) OR (user NEAR/3 accountability) OR (consumer NEAR/3 accountability) OR (citizen NEAR/3 accountability) OR (personal NEAR/3 accountability) OR (individual NEAR/3 accountability) OR (user NEAR/3 agenc*) OR (consumer NEAR/3 agenc*) OR (citizen NEAR/3 agenc*) OR (personal NEAR/3 agenc*) OR (individual NEAR/3 agenc*) OR (self-censor*) OR ("self censor*") OR (self NEAR/3 censor*)	privacy OR secur* OR safe* OR protect* OR private	meta-analy* OR "systematic review" OR (design or study or analysis) OR intervention* OR ("quasi experiment*" or "quasi-experiment*") OR experiment*

APPENDIX B: DATABASE SEARCH QUERIES

ProQuest

ti(((user NEAR/3 responsibility) OR (consumer NEAR/3 responsibility) OR (citizen NEAR/3 responsibility) OR (personal NEAR/3 responsibility) OR (individual NEAR/3 responsibility) OR (user NEAR/3 accountability) OR (consumer NEAR/3 accountability) OR (citizen NEAR/3 accountability) OR (personal NEAR/3 accountability) OR (individual NEAR/3 accountability) OR (user NEAR/3 agenc*) OR (consumer NEAR/3 agenc*) OR (citizen NEAR/3 agenc*) OR (personal NEAR/3 agenc*) OR (individual NEAR/3 agenc*) OR ("self-censor*") OR ("self censor*") OR (self NEAR/3 censor*))) OR ab(((user NEAR/3 responsibility) OR (consumer NEAR/3 responsibility) OR (citizen NEAR/3 responsibility) OR (personal NEAR/3 responsibility) OR (individual NEAR/3 responsibility) OR (user NEAR/3 accountability) OR (consumer NEAR/3 accountability) OR (citizen NEAR/3 accountability) OR (personal NEAR/3 accountability) OR (individual NEAR/3 accountability) OR (user NEAR/3 agenc*) OR (consumer NEAR/3 agenc*) OR (citizen NEAR/3 agenc*) OR (personal NEAR/3 agenc*) OR (individual NEAR/3 agenc*) OR ("self-censor*") OR ("self censor*") OR (self NEAR/3 censor*)))

AND

ti((privacy OR secur* OR safe* OR protect* OR private)) OR ab((privacy OR secur* OR safe* OR protect* OR private))

AND

ti((social NEAR/3 media) OR ("online social network*") OR (social NEAR/3 networking NEAR/3 site*) OR ("online platform*") OR ("digital platform*") OR (internet) OR (cyber)) OR ab((social NEAR/3 media) OR ("online social network*") OR (social NEAR/3 networking NEAR/3 site*) OR ("online platform*") OR ("digital platform*") OR (internet) OR (cyber))

AND

ti((meta-analy* OR "systematic review" OR design or study or analysis OR intervention* OR "quasi experiment*" or quasi-experiment* OR experiment*)) OR ab((meta-analy* OR "systematic review" OR design or study or analysis OR intervention* OR "quasi experiment*" or quasi-experiment* OR experiment*))

Scopus

TITLE-ABS-KEY (((user W/3 responsibility) OR (consumer W/3 responsibility) OR (citizen W/3 responsibility) OR (personal W/3 responsibility) OR (individual W/3 responsibility) OR (user W/3 accountability) OR (consumer W/3 accountability) OR (citizen W/3 accountability) OR (personal W/3 accountability) OR (individual W/3 accountability) OR (user W/3 agenc*) OR (consumer W/3 agenc*) OR (citizen W/3 agenc*) OR (personal W/3 agenc*) OR (individual W/3 agenc*) OR ("self-censor*") OR ("self censor*") OR (self W/3 censor*)))

AND

TITLE-ABS-KEY ((privacy OR secur* OR safe* OR protect* OR private))

AND TITLE-ABS-KEY ((social W/3 media) OR ("online social network*") OR (social W/3 networking W/3 site*) OR ("online platform*") OR ("digital platform*") OR (internet) OR (cyber))

AND (meta-analy* OR "systematic review" OR design or study or analysis OR intervention* OR "quasi experiment*" or "quasi-experiment*" OR experiment*)

Web of Science

TOPIC: ((user NEAR/3 responsibility) OR (consumer NEAR/3 responsibility) OR (citizen NEAR/3 responsibility) OR (personal NEAR/3 responsibility) OR (individual NEAR/3 responsibility) OR (user NEAR/3 accountability) OR (consumer NEAR/3 accountability) OR (citizen NEAR/3 accountability) OR (personal NEAR/3 accountability) OR (individual NEAR/3 accountability) OR (user NEAR/3 agenc*) OR (consumer NEAR/3 agenc*) OR (citizen NEAR/3 agenc*) OR (personal NEAR/3 agenc*) OR (individual NEAR/3 agenc*) OR ("self-censor*") OR ("self censor*") OR (self NEAR/3 censor*))

AND

TOPIC: ((privacy OR secur* OR safe* OR protect* OR private))

AND

TOPIC: ((social NEAR/3 media) OR ("online social network*") OR (social NEAR/3 networking NEAR/3 site*) OR ("online platform*") OR ("digital platform*") OR (internet) OR (cyber))

AND

TOPIC: ((meta-analy* OR "systematic review" OR design or study or analysis OR intervention* OR "quasi experiment*" or "quasi-experiment*" OR experiment*))

APPENDIX C: PROQUEST SUBJECT TERMS

(subt.exact("internet" OR "social networks" OR "studies" OR "privacy" OR "consumers" OR "censorship" OR "computer security" OR "digital media" OR "social media" OR "communication" OR "ethics" OR "social responsibility" OR "surveillance" OR "accountability" OR "computer software" OR "consumer behavior" OR "consumer protection" OR "decision making" OR "economics" OR "personal information" OR "research" OR "society" OR "web sites" OR "access to information" OR "behavior" OR "citizen participation" OR "citizens" OR "communications technology" OR "information management" OR "information technology" OR "internet access" OR "qualitative research" OR "researchers" OR "smartphones" OR "social aspects" OR "social research" OR "systematic review" OR "user behavior" OR "virtual organization" OR "young adults" OR "adolescent" OR "adult")