The Journal of Systems & Software 200 (2023) 111620

Contents lists available at ScienceDirect

The Journal of Systems & Software

journal homepage: www.elsevier.com/locate/jss

People want reassurance when making privacy-related decisions — Not technicalities☆

Oksana Kulyk [a,*], Karen Renaud [b,c,d,e], Stefan Costica [b]

[a] IT University of Copenhagen, Copenhagen, Denmark
[b] University of Strathclyde, Glasgow, United Kingdom
[c] Rhodes University, Grahamstown, South Africa
[d] University of South Africa, Pretoria, South Africa
[e] Abertay University, Dundee, UK

ARTICLE INFO

Article history:
Received 7 April 2022
Received in revised form 24 November 2022
Accepted 16 January 2023
Available online 10 February 2023

Keywords:
Cyber
Privacy
Decision-making
Reassurance

ABSTRACT

Online service users sometimes need support when making privacy-related decisions. Humans make decisions either slowly, by painstakingly consulting all possible information, or quickly, by relying on cues to trigger heuristics. Human emotions elicited by the decision context affects decisions, often without the decision maker being aware of it. We wanted to determine how an information-based decision can be supported, and also to understand which cues are used by a heuristics-based approach. Our first study enhanced understanding of underlying encryption mechanisms using metaphors. Our participants objected to efforts to make them 'technical experts', expressing a need for reassurance instead. We fed their free-text responses into a Q-sort, to determine which cues they rely on to make heuristic-based decisions. We confirmed the desire for reassurance. Our third study elicited 'cyber stories': Unprompted narratives about cyber-related experiences to detect emotional undertones in this domain. Responses revealed a general negativity, which is bound to influence cybersecurity-related decisions.

© 2023 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

The GDPR regulation[1] is intended to give European Union and UK citizens the right to have their privacy respected, with punitive fines applied to companies who fail to do so. Other countries have similar legislation. GDPR mandates that citizens be permitted to decline or agree to divulge their information. The Information Commissioner in the UK classifies some kinds of data as 'sensitive', and this includes health data. This paper reports on how decisions to divulge health data are made and can be supported from a privacy perspective. There are two ways people make decisions: information-based (System 2) and heuristic-based (System 1) (Kahneman, 2011).

Information-based: There is an implicit assumption that people can only make a truly informed decision if they have all the information to hand (Bekker et al., 1999). Indeed, this assumption is hinted at in the almost ubiquitously used term related to gaining consent to harvest data: "informed decision making". This is why voluminous 'Terms and Conditions' documents are provided to online users (Jensen and Potts, 2004; Schaap et al., 2020; Betzing et al., 2020). Making fully informed decisions is a complex, cognitively demanding and time-consuming activity (Acquisti et al., 2007; Solove, 2013) but much of what we do online, in obtaining consent, is based on this paradigm. The question is whether exhaustive and comprehensive information really informs decision making in the privacy realm.

Heuristics-based: Users rely on heuristics which are activated by specific influential cues to reduce the inherent complexity and time-consuming nature of decision making. In doing so, they rely on what they already know and what they can gauge from the environment, very quickly and efficiently. They will rely on specific cues, which include (Bekker et al., 1999): the look and feel and features of the user interface, pre-existing trust in the website owner or brand, and the privacy- and security-related assurances displayed by the website (Sunstein and Thaler, 2014).

Emotion: Both information- and heuristics-based decisions will be influenced by the person's own underlying emotions towards the context within which the decision is made (Bekker et al., 1999), in this case cybersecurity. Initial forays into cybersecurity-related emotions suggest a general negativity (Renaud et al., 2021), which is likely to lead to avoidance (Allidina and Cunningham, 2021), exactly the opposite of what a privacy-related decision requires.

☆ Editor: Raffaela Mirandola.

* Corresponding author.
E-mail addresses: okku@itu.dk (O. Kulyk), karen.renaud@strath.ac.uk (K. Renaud), stefan.costica99@gmail.com (S. Costica).

[1] https://www.gov.uk/government/news/gdpr-is-here.

https://doi.org/10.1016/j.jss.2023.111620
0164-1212/© 2023 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

Many privacy-related studies focus on providing comprehensive information to inform privacy-related decisions (e.g., Scott et al., 2003). Others investigate the role of heuristics in privacy-related decision making (e.g., Sundar et al., 2020). A third group have investigated emotion in cybersecurity (e.g., Renaud et al., 2021). This is the first study to bring all three of the aspects to a single study of privacy-related decision making in the health data context. We report on three studies in this paper, to explore each of the decision-making aspects mentioned above. As such, the contribution of this paper are:

1. The finding that people do not want to be informed of how the underlying technical cybersecurity mechanisms work i.e., they do not want to become 'technical experts'.
2. People rely primarily on reassuring statements in deciding whether or not to divulge their health data i.e., they make use of cues to inform their heuristics, and reassuring statements are particularly influential.
3. Many people feel generally negative about cybersecurity, confirming previous findings (Renaud et al., 2021) i.e., they often experience negative cybersecurity-related emotions, and this might lead to avoidance of decision making and to general scepticism of the extent to which online service providers can be trusted.

We commence by reviewing the research literature, then we introduce the research questions we plan to answer with our studies. After presenting the studies in Sections 3, 4 and 5, Section 6 discusses and reflects on our findings. Section 7 concludes.

2. Related research & research questions

2.1. Privacy

Privacy is a fundamental human right (Equality and Human Rights Commission, 2021), which came into existence after the second World War (Diggelmann and Cleis, 2014). In accordance with the universal right to privacy, people have the right to consent before their personal information is collected and used.

A great deal of work has been undertaken to study privacy. For example, Westin attempted to classify population-level privacy stances (Westin, 2003), others have studied the influence of thinking styles on privacy decisions (Kehr et al., 2015), and yet others consider how to encourage people to read privacy policies (Aïmeur et al., 2016).

Privacy is challenging to study because of the privacy paradox. This phenomenon suggests a lack of agreement between expressed privacy concerns and actions people actually take to protect and preserve their privacy (Kokolakis, 2017). Some researchers have carried out studies that seem to confirm the existence of the paradox (Dienlin and Trepte, 2015; Barth et al., 2019; Li et al., 2017). Yet, a number of other researchers argue that the paradox is an artefact of the way the experiments are carried out (Gruzd and Hernández-García, 2018; Solove, 2020; Hong et al., 2019; Jozani et al., 2020). They argue that people are asked about their privacy concerns in a general way, but that their actions are tested in a context-sensitive format, suggesting a paradox. Such inconsistencies could easily lead to the conclusion that people do not really value their privacy. Given the disagreement with respect to the existence of this paradox, it is worth exploring whether people do indeed care about the privacy of their information. In particular, we need to understand how people make privacy-related decisions.

2.2. Enhancing comprehension

To improve comprehension, we can either provide a great deal of text, or a visual element. In particular, visual metaphors can help people to understand complex and abstract concepts (Trepagnier, 2019; Ward, 2010), and the prevalence metaphors of cybersecurity in public discourse has been noted by several authors (Branch, 2021; Karas et al., 2008; Canbek, 2018; Betz and Stevens, 2013; Lawson, 2012; Lapointe, 2011). Raja et al. (2011) compared three metaphors to convey firewall principles. They discovered that a metaphor relating a software firewall to a physical wall with a metal door was the most effective in enhancing comprehension. Raja et al. explain that pictorial metaphors can be very powerful in conveying risk to computer users. Skrynnikova (2020) reports that metaphor co-creation can be useful in improving the quality of cybersecurity metaphors, in terms of maximising their ability to communicate complex concepts.

It is certainly important to ensure that metaphors do indeed increase understanding (Thibodeau et al., 2019) and do not engender misunderstandings (Lapointe, 2011; Taylor and Dewsbury, 2018). Thorough testing of metaphors is essential (Wästlund et al., 2011). An example of such testing is a study by Demjaha et al. (2018) that investigated the impact of metaphors on users' understanding of threat models behind instant messengers with end-to-end encrypted communication, investigating such metaphors as special language, treasure hunt (with the secret key as a metaphor for a treasure map), colours (with the secret key as a metaphor for a secret colour that allows to "unmix" the exchanged messages), banknotes (as something initially unusable by being ripped in half, but that can be matched if halves are combined), and owl (as someone who will only deliver the message to the intended recipient). Their results demonstrate that metaphors do not always foster understanding of the threat model. In essence, metaphor efficacy cannot be assumed. In some cases, their use leads to an overestimation of security guarantees that techniques such as end-to-end encryption can provide (e.g., believing that someone who gains access to the endpoint (user's phone) will not be able to read their messages).

2.3. Heuristics & Cues

Mazurek and Małagocka (2019) suggest that people will disclose personal information based on three T's: (1) *transparency*, (2) *type of data*, and (3) *trust*. The first is related to the communication between the parties and the procedures used. The second is based on the type of data being shared. The third is related to the person's trust in the brand and the value that the person gains from divulging their personal information.

When using heuristics, people will rely on cues that signal the existence of those three T's (Bhuiyan et al., 2021; Wang and Emurian, 2005; Olausson, 2018). If the cues signal trust, then uncertainty, perceived risk and randomness is reduced (Beldad et al., 2012; Kim and Kim, 2018; Xie et al., 2006; Kulyk et al., 2020).

The presence of various security and privacy assurances (such as security or privacy seals or statements) and the level of control provided to the user, impacts data disclosure and privacy concerns (Becker et al., 2020; Coles-Kemp and Kani-Zabihi, 2010; Kim and Kim, 2018).

2.4. Emotion & decision making

Emotions are short-lived and relatively intense experiences, which colour perceptions, influence decisions, and trigger behaviours (Shouse, 2005; Martin et al., 1993). The cybersecurity

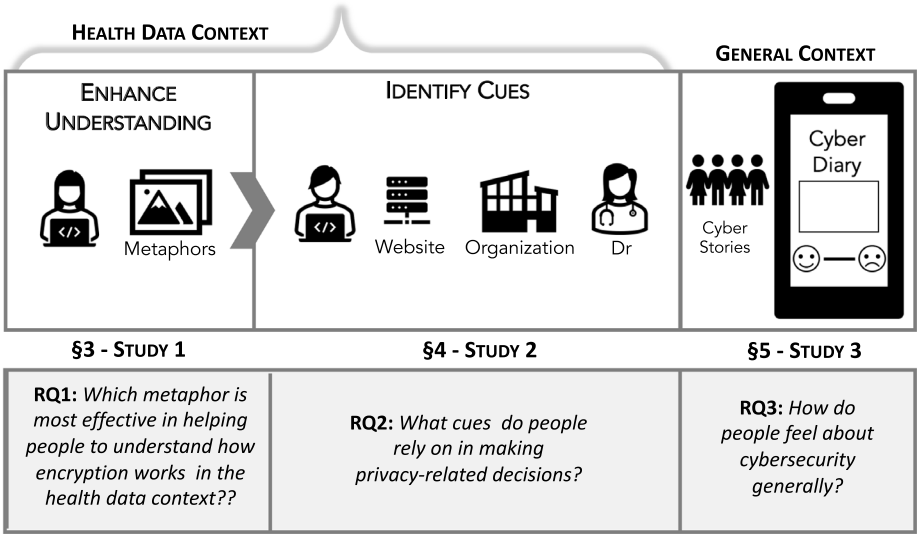

Fig. 1. Studies 1, 2 & 3.

context is alive with events that can trigger emotional responses, both negative and positive. Renaud et al. (2021) reveal a negative tone towards cybersecurity but argue that their results are not yet sufficient to inform behavioural interventions.

What we *do* know is that if people feel positivity, they will approach, and if they feel negativity, that will withdraw and avoid (Maio and Esses, 2001). When it comes to cybersecurity, avoidance is undesirable. By implication, we should try to eliminate negativity to encourage engagement.

2.5. Research questions & motivation

To test the first type of decision making, we will test metaphors to improve comprehension of encryption, which few people really understand (Dechand et al., 2019). This is relevant because privacy is usually assured by means of encryption, We chose to improve comprehension by using a variety of metaphors, given their propensity for maximising comprehension of complex topics (Morgan and Reichert, 1999; Thibodeau and Durgin, 2008).

This leads us to the first research question: "*RQ1: Will a metaphor be effective in helping people to understand how encryption works?*" Investigating RQ1 has two purposes: (1) to identify the best metaphor, and (2) to test whether people do indeed want to improve their understanding of complex cybersecurity mechanisms.

If people use heuristics, they will rely on specific cues in the choice architecture to make decisions. This leads to the second question: "*RQ2: What cues do people rely on in making privacy-related decisions?*"

The third research question explores general emotions related to cybersecurity: "*RQ3: How do people feel about cybersecurity generally?*"

Fig. 1 depicts the three studies reported on in this paper.

3. Study 1 - Privacy decision rationalisations

RQ1: *Will a metaphor be effective in helping people to understand how encryption works?*

3.1. Materials

The first study presents a scenario of a health tracker app that provides the option either to share health data with a healthcare provider, or to keep it locally on their own smartphone. The users are shown a metaphor to highlight the protection afforded by encryption during data transmission to a trusted healthcare provider. We selected three metaphors and assigned participants randomly to one of the following: *(1) Lock and Key:* presenting encrypted data as being locked inside a safe, and the key to the safe is only possessed by the authorised entity (Fig. 2). *(2) Language* depicting encrypted data as being translated into a secret unique language, with only authorised entities being able to understand it. (Fig. 3). *(3) Vault:* presenting encrypted data as being put into a vault (similar to the lock-and-key metaphor), which is depicted as being impervious to a hacker's attempts to extricate the contents of the message (Fig. 4)

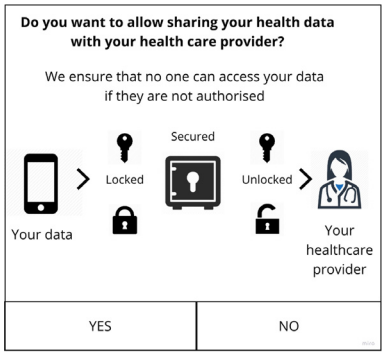

Fig. 2. Lock & key metaphor.

3.2. Study procedure

The study was a between-subjects online survey, with participants recruited via the Prolific platform.[2] Participants were paid £1.25 for an estimated 10 min of labour, exceeding the UK minimum wage. As the data collecting author's institution does not require a mandatory ethical approval, no ethical review board was consulted. Nonetheless, we took care to minimise harm to participants by ensuring their informed consent and anonymity of responses.

2 https://www.prolific.co/.

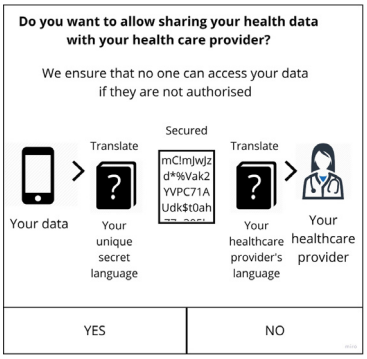

Fig. 3. Language metaphor.

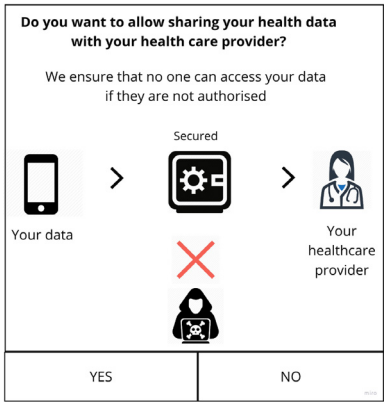

Fig. 4. Vault metaphor.

Before commencing, participants were presented with a consent form, outlining the purpose of the study and assuring them of the anonymity of their responses. They were presented with a description of the health tracker app and a visual representation of a corresponding randomly-assigned metaphor. They were asked to indicate their willingness to share their health data and their understanding of the level of security the app provides.

Afterwards, participants were asked which of the following kinds of information they would like to see: "*A personal endorsement from a well known cyber security expert*", "*Information about app compliance with standards and regulations*" or "*Reviews from other users of the app*" (for the full list see the Appendix). They were asked to rate usefulness of each on a 5-point Likert scale, from "not useful at all" to "very useful".

In the final part of the study, the participants were shown a list of assurances (e.g. "*We ensure that your data is protected by having our services certified according to the ISO/IEC 27001 information security standard.*"). We then asked whether such an assurance would make it more likely that they would share their data, and requested elaboration.

3.3. Hypotheses

We consider at following hypotheses:

H1: There is a difference between metaphors, in terms of how likely the participants would be to share their data.

H2: There is a difference between metaphors, in terms of how well the participants understand the security model.

H3: There is a difference between different types of information, in terms of how useful the participants find it for deciding whether to share their data, or not.

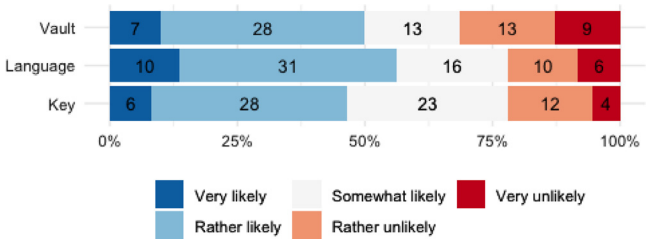

Fig. 5. Willingness to disclose data based on metaphor.

H4: There is a difference between different assurances, in terms whether the assurance would make the participants more likely to share their data.

3.4. Results

217 participants completed our survey (133 male, 83 female and one non-binary). 70% were between 20 to 35 years of age. As the consequence of random assignment, 70 participants were allocated to the "Vault" group, 73 to the "Lock and Key" group and 74 to the "Language" group.

The statistical analyses described in this section have been performed using R packages "stats", "PMCMR", "coin".

Willingness to share data: Overall, 51% of participants were either "rather likely" or "very likely" to share data. Fig. 5 shows the distribution of participants' scores, depending on their assigned metaphor. There was no significant difference between the groups (using Pearson chi-squared test Agresti, 2003, $\chi^2(2, N = 216) = 1.6294$, $p = .443$). **H1 was not confirmed**. The participants varied in their willingness to share data depending on the purpose (see Fig. 6), the significant differences were confirmed via the Friedman test (Hollander and Wolfe, 1973) ($\chi^2(8, N = 215) = 434.59$, $p < .001$, effect size $W = .253$, small). The post-hoc Nemeniy tests (Nemenyi, 1963) do not reveal any differences in willingness to disclose data for a particular purpose depending on the metaphor (p-values adjusted using Benjamini–Hochberg method Benjamini and Hochberg, 1995 ranging from .678 to .825).

Participants varied in their willingness to share data depending on the purpose (see Fig. 6). The purposes rated as most likely to lead to sharing were "*Being able to easily provide a report for your doctor's use*", "*Helping with medical research*" and "*Getting personalised advice about improving your health", (rated as either "very compelling*" or "*rather compelling*" by 70%, 60% and 57% of participants, respectively). The purposes that were rated as least likely to lead to data sharing were "*Getting personalised ads*", "*Getting regular updates about ongoing situations e.g. with the COVID-19 pandemic*", "*Getting a personalised COVID-19 risk assessment*" (rated as either "*very compelling*" or "*rather compelling*" by 12%, 39% and 48% of participants respectively). An overview of ratings for all the purposes is provided in Fig. 6.

Understanding of security model: The mean number of correct answers was 2.41 (out of maximum of 5), with a standard deviation of 1.15. The number of participants who gave correct answers regarding individual threats is provided on Table 1. While most of the participants correctly answered that an adversary who succeeds in guessing the phone password and is able to hack into their phone or access the server would have access to their health data (140/139/119). The rest of the threats were less well understood. In particular, only 36% of participants correctly answered that an adversary controlling the network communication would not be able to obtain their health data (with other chosen answers almost evenly split, i.e. 22% answering that an attacker would succeed in obtaining one's health data,

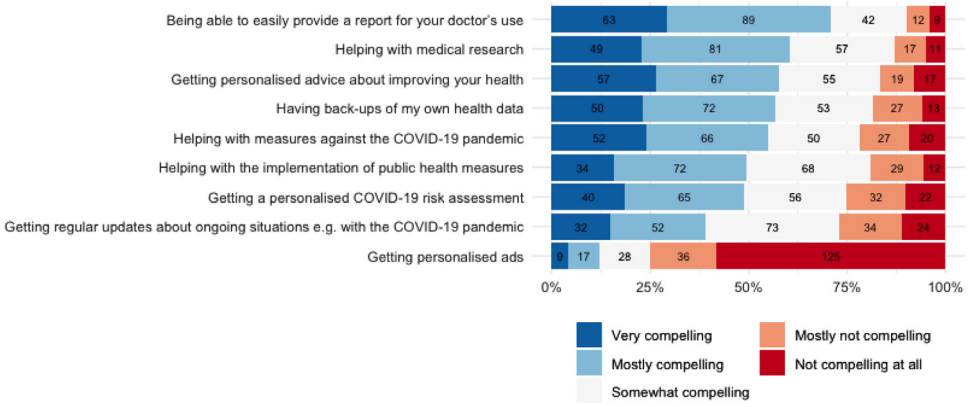

Fig. 6. Willingness to disclose data based on purpose.

Table 1
Number of participants providing a correct answer to each of the threats.

Threat	Correct answer	# Correct
Insurance companies can access your health data	More information needed	49
Someone who eavesdrops on the network communications sent and received by the app can obtain your health data	False	79
Someone who guesses the password you use to unlock your phone can access your health data	True	140
Someone who hacks into your phone can access your health data	True	136
Someone who hacks into the health app server can access your health data	True	119

23% believing that additional information would be required to answer that question, and 18% did not know). Furthermore, only 22% correctly answered that additional information would be required to tell whether insurance companies would have access to their health data. The most popular answer (chosen by 38%) being that they would not be able to do so, followed by the answer that the statement was true (22%) or "don't know" (17%).

The mean number of correct answers was 2.23 for the participants assigned to the "vault" metaphor (standard deviation 1.16), 2.37 for the ones assigned to the "key" metaphor (standard deviation 1.23) and 2.62 for the ones assigned to the "language" metaphor (standard deviation 1.06). There was no significant difference between the metaphors (ANOVA Chambers et al., 2017, $F(2, 214) = 2.17$, $p = .117$) in terms of number of correct answers. **H2 was not confirmed**.

Fig. 7 shows the percentage of correct answers for each threat, depending on the assigned metaphor. The "language" metaphor performed better than the "vault" and "key" metaphors for several threats. Most prominently, 51% of participants correctly answered that an attacker controlling the network would not be able to obtain the communicated health data. Only 24% and 33% of participants in the "vault" and "key" groups, respectively, provided the correct answer to this question. The pairwise tests show significant differences in the percentage of correct answers for the "network" threat depending on the assigned metaphor (Pearson chi-squared test, $\chi^2(2, N = 217) = 11.974$, $p = .003$[3]). However, the same does not apply to other threats (adjusted p-values ranging from .399 to .797).

3.4.1. Usefulness of provided information

Overall, 51% of participants answered that they were either "rather likely" or "very likely" to share data. Nonetheless, 85% responded that they wanted additional information before making a decision. When asked to rate the usefulness of different types of information, the top rated were "*Information about what data is shared with third parties*", "*Information about what data is collected by the app developers*", "*Information about app compliance with standards and regulations*" (rated as either "very useful" or "mostly useful" by 80%, 75% and 69% of participants, respectively). The types of information rated to be least useful were "*Technical details about the app*", "*Information about the app developer*"' and "*A personal endorsement from a well known cyber security expert*" (rated as either "very useful" or "mostly useful" by 43%, 43% and 51% of participants respectively). An overview of ratings for specific types of information is provided in Fig. 8. There are significant differences between the rated usefulness of different types of information (Friedman test, $\chi^2(7, N = 209) = 254.13$, $p < .001$, effect size $W = .174$, small),[4] **confirming H3**.

3.4.2. Assurances

The majority of participants felt that assurances would make them more likely to disclose their data (rating them as "slightly more likely", "more likely" or "much more likely"). Others felt that the assurances would not change anything. An overview of ratings is provided in Fig. 9. There is a significant difference between the assurances (Friedman test, $\chi^2(4, N = 217) = 22.411$, $p < .001$, effect size $W = .0258$, small),[5] **confirming H4**. The most powerful assurances "*We ensure that your data is protected by complying with the relevant legal regulations, such as the GDPR*", "*We ensure that your data is protected by having our services certified according to the ISO/IEC 27001 information security standard*" and "*This app has been tested by a team of ethical hackers, who found no vulnerabities*" (rated as either "much more likely", "more likely" or "slightly more likely" by 62%, 55% and 55% of participants, respectively).

The assurances rated as least likely to lead to data disclosure were "*We do not share your personal data. We may share the data you provide in anonymized aggregated format with our partners in order to improve our services*", "*This app has been tested by a team of ethical hackers, who found no vulnerabities" and "We ensure that your data is protected by having our services certified according to the ISO/IEC 27001 information security standard*" (rated as either

[3] $p = .01$ after adjusting for multiple comparisons using the Benjamini–Hochberg method.

[4] The post-hoc tests describing differences between information types are provided in the Appendix, see Table A.2.

[5] The post-hoc tests describing differences between assurances are provided the Appendix, see Table A.3.

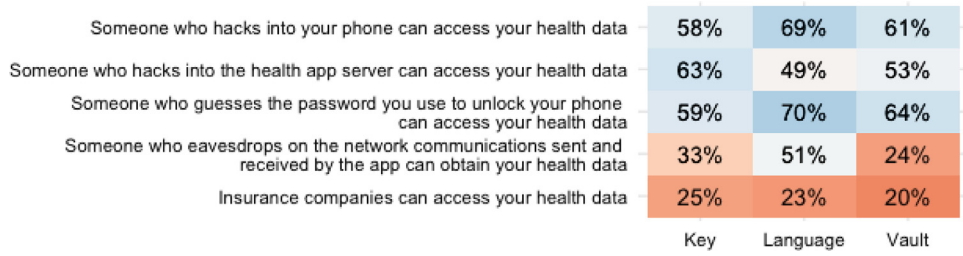

Fig. 7. Percentage of participants providing a correct answer for each threat, depending on the assigned metaphor.

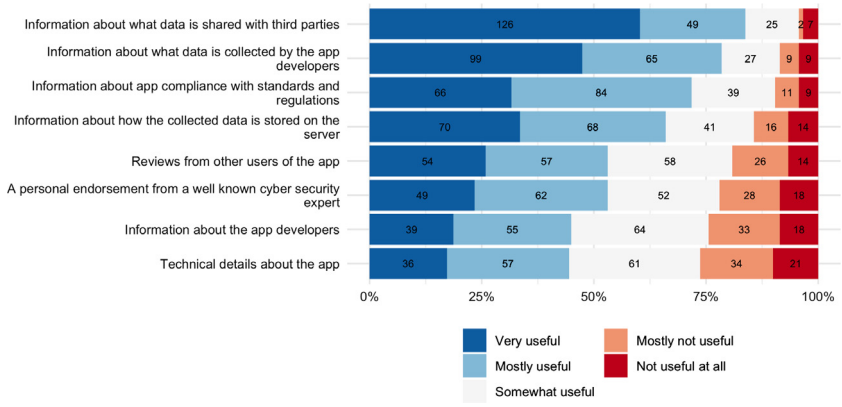

Fig. 8. Perceived usefulness of various types of information.

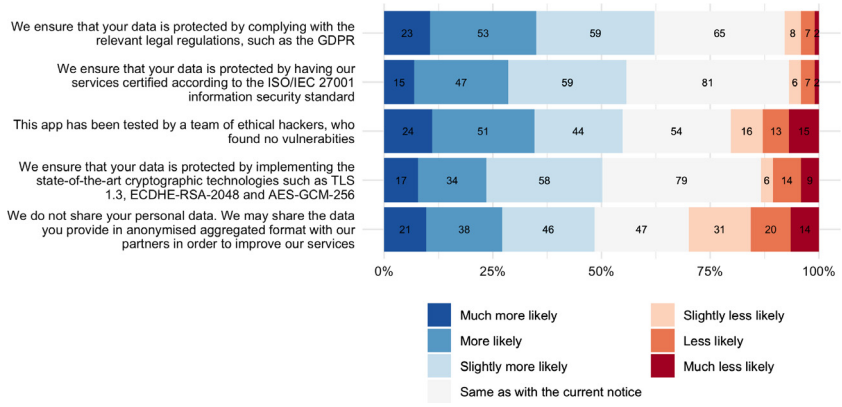

Fig. 9. Perceived likelihood of various types of assurances to lead to data disclosure.

"much less likely, "less likely", "slightly less likely" by 30%, 20%, 13% of participants, respectively).

The free-text responses explaining rankings were analysed via open coding, with two authors performing the coding and resulting in Cohen's Kappa of 0.77 (substantial) (McHugh, 2012). Excluding participants who did not provide any response, as well as responses that were unclear, a total of 191 responses were coded. The following codes were derived:

Confusion/Uncertainty: They expressed uncertainty regarding the protection of their data, stating that they did not have sufficient understanding of security as a whole nor of specifically mentioned technologies/standards: "*I do not know enough about cyber security for these descriptions to mean very much to me.*"

Understandable Information They wanted information about data protection, stressing the need for this to be clear and understandable: "*I think that it's better to say to the customer something that he can easily understand*".

Importance of Data Protection: The participants confirm the importance of data protection to them: "*The most important think for me its my data security*".

Importance of Assurances: The participants express the wish from either service providers or third-party experts to reassure them regarding the security of their data: "*I just want to know that my data is protected*".

Mistrust/Cynicism: They expressed distrust regarding the genuineness of the statements or regarding the extent to which stated protections can indeed be effective: "*I have little trust in general when it comes down to data collecting from private companies and the message itself would do little to improve that opinion.*"

Reliance on Legal Standards: The participants stress the importance of legal compliance – most importantly, GDPR compliance – as a way to ensure accountability: "*I feel more*

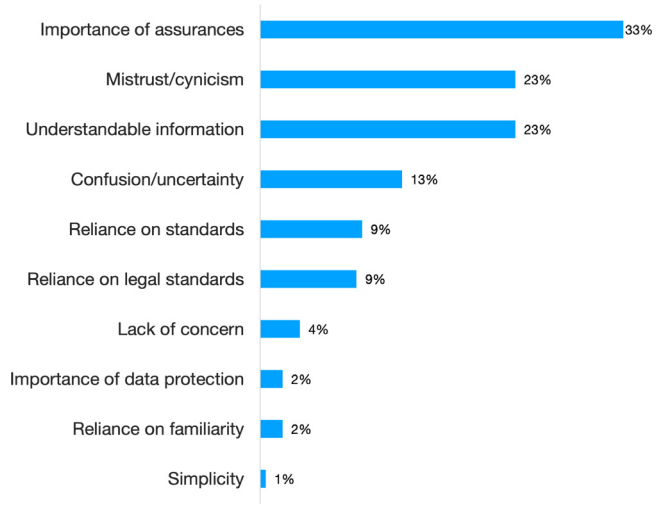

Fig. 10. Percentage of participants (out of total 191 whose responses were coded) mentioning each code.

secure using the app knowing that I'm protected by my country's laws and international security regulators."

Reliance on Familiarity: The participants express positive attitudes towards protection measures that they are familiar with: "*I guess them attesting to regulations that I recognise would make me more likely to trust them*".

Reliance on Standards: The participants report having trust in established standards and regulations: "*I think if the information is regulated by any globally recognised standard it is safe*".

Lack of Concern: The participants reported not being concerned over data sharing, regardless of the statements: "*i have nothing to hide, so I am ok since the beginning in install this app*".

Desire for Simplicity: The participants stated the preference for simpler and concise statements. "*I think that less is better*".

Fig. 10 shows the relative frequency of codes. In particular, the two most common codes were "importance of assurances" (mentioned by 33% participants), followed by the desire for clear and understandable information and mistrust (each mentioned by 23% participants).

3.5. Deriving the Q-statements

The outcome of the first study will feed into the second study. We thus needed to derive Q-statements to facilitate Q-sorting. We relied on the free-text responses provided by the participants, given that these reflected *their* perceptions about what would encourage them to divulge their heath information.

Two of the paper authors worked through the comments provided by the participants independently to extract reasons for, and against, divulging health information online. We reformatted these into statements which we could use in the Q-sort procedure. We did this independently then met to refine and agree on final statements. Initial disagreements were resolved via discussion, in which we refined our definitions of the codes and came up to a common understanding on how individual statements should be coded. The authors then worked through the list together to combine semantically similar statements to gauge public perceptions of the extent to which the different reassuring statements allayed scepticism. The final statements are provided in Table A.4 in Appendix.

The statements reflect a mixture of influences: (1) individual rationalisations (e.g., 16 & 20), (2) reassurance statements (e.g., 36 & 37), and (3) observations based on their assessment of the website features (e.g., 12 & 19). The classification is indicated by 1, 2 or 3 subscripts next to each statement in Table A.4.

4. Study 2 - cues

RQ2: "*What cues do people rely on in making privacy-related decisions?*"

4.1. Methodology

A decision to divulge information is inherently subjective, and it is important to understand people's thinking in this respect. We used Q-methodology, a research method introduced by Stephenson (1935), to support the systematic study of subjectivity. Q-methodology provides a framework for measuring beliefs *as cultural phenomena*. The findings from a Q-methodology analysis reveal the *nature* of subjectivity: '***what** is the nature of different groups' thinking?*', as opposed to '***how** are people thinking on the topic?*'. This methodology considers large numbers of participants to be '*relatively unimportant*' (Brown, 1993).

Q-methodology reveals correlations between subjects across a sample of variables, referred to as the "Q-set" that is composed of 'Q-statements'. Factor analysis isolates the most influential "factors", which represent cultural ways of thinking. The method's strength is that it applies sophisticated factor analysis, supporting qualitative analysis. It also elicits free-text responses allowing people to explain why they agree or disagree with different statements. It is not designed to prove or disprove hypotheses, but rather to provide a sense of '*potentially complex and socially contested*' issues (Watts and Stenner, 2005). Fig. 11 depicts the steps involved in a Q-sort.

Participants sort Q-Statements into a fixed quasi-normal distribution, ranging from −3 (disagree) to +3 (agree). Participants were given a chance to amend and confirm their rankings and then asked for open-ended comments for the most agreed with (ranked +3) and most disagreed with (ranked −3) statements. This serves to gain '*an impression of the range of opinion at issue*' (Brown, 1993).

4.2. Study procedure

Similar to Study 1, the participants for the study were recruited via the Prolific platform and paid £5 for an estimated 30 min of labour, exceeding the UK minimum wage. As with Study 1, no ethical board was consulted due to lack of such a requirement on behalf of the data collecting author's institution, and measures to ensure informed consent and confidentiality of participants' responses were implemented.

Participants were given the following scenario: "*A website is asking for your health information. What would make you likely to provide it?*" Five pilot tests were undertaken and timed, to determine how long it took to carry out the task. Based on feedback obtained from the pilot testers, unclear statements were refined and clarity improved.

Forty participants were recruited on the Prolific platform. This is consistent with recommended participant group sizes in Q-methodology (Watts and Stenner, 2005). Twelve of the participants were female, 27 were male and one person did not specify their gender. The mean age of the participants was 28.05 years. Based on the pilot study timings, we paid participants £5 for 30 min of labour, exceeding the UK minimum wage. Participants did not provide any personal data, ensuring that participation was anonymous.

Fig. 11. Q-sorting process.

4.3. Results

We extracted factors using the principal component extraction technique and applied a varimax procedure for factor rotation. Factors with an eigenvalue in excess of 1.00, and having at least two significantly loading participants, were selected for interpretation (as recommended by Watts and Stenner, 2005) (Fig. A.15). Factors 3 and 5 were eliminated because they had only 1 participant.

Factor 1: Appreciate being given more control and want information to make an informed decision:

Demographic information: Factor 1 has 11 significantly loading participants (6M/5F) with an average age of 29.2 years. It explains 34% of the study variance with an eigenvalue of 13.53.

Factor interpretation: There is a clear need amongst this group for a sense of control: "*There may be some things I am happy to share and some I'm not, so greater control is appealing*" and "*I need to know I'm safe and protected and will check I won't take anyone's 'word for it'*". This group do not avoid reading the provided information: "*it is important to read all the information available so that you know what you are consenting to*". They strongly disagreed with any suggestion that they did not want assurances about encryption: "*I have no reason to not believe their claims, so as long as as the website is well reviewed I would have no issue placing my trust in them*". They did not agree with the statements: "*Life is too short to read all this information*" and "*It doesn't matter what I see. I will share my information*". This confirms the findings from the first study related to people's need for information to help them make decisions.

Factor 2: Want extra assurance and reassurance, and are discriminating about what information they share:

Factor 2 has 3 significantly loading participants (2M/1F) with an average age of 23.7 years. It explains 7% of the variance.

Factor interpretation: These participants liked the idea of two factor authentication: "*Two-factor authentication guarantees that, even if the website, a hacker or someone else gains access to my password, they cannot access my account, they would need access to my phone for that.*" They are also very sceptical about the efficacy of anonymisation mechanisms: "*Companies might try to make you feel you are completely anonymus when you are not. I feel that this happens a lot with social networks for example. People feel safe with them, but they are not. You cant be 100% anonymus on the internet, so thats why i wont trust someone that tells me i will be anonymus using their website/services.*".

They do not avoid reading information: "*Reading the information a website provides is crucial to know if they are trying something shady, or they just want you to accept some terms thinking you wont even read the consent forms. Thats why i always read and search as much information as possible about a website before feeling 'secure'*". There is also a great desire to understand what the website is going to do with their information: "*Im not an expert about internet security, although I think i defend myself on this field. Thats why I try my best to keep myself updated about internet security, to avoid being fooled*".

Factor 4: Have faith in experts, and need evidence that they have underwritten the website:

Factor 4 has 3 significantly loading participants (3M/0F) with an average age of 20.3 years. It explains 5% of the variance.

Reassurance from experts convinces these participants: "*Having a 'thumbs up' from security experts does show you have good security measures*" and they like to get extra information "*I prefer that The website provides a link to extra information about its security and privacy assurance practices because it seems more professional*".

They certainly did not trust websites simply because they did not understand security: "*Just because you dont understand doesnt mean you have to trust, it's that simple*". Moreover, they definitely pause to consider, not automatically sharing their information: "*Couldnt disagree more, you should NEVER share information without first reading what info they want and for what for*" and "*I take my information very seriously and I would rather read the information that they are willing to give me so that I could make a proper decision on my own part.*"

Factor 6: Want to see assurances about data sharing, but are not taken in by aesthetics:

Factor 6 has 2 significantly loading participants (2M/0F) with an average age of 20.5 years. It explains 4% of the variance.

These participants are reassured by statements related to data sharing: "*They are usually(?) unbiased and have little gain in lying about security*" and "*if the website has some statements from expert, maybe the website result more confident*". Yet, they were not reassured by the website testing assurances: "*in my opinion a website has always some vulnerabilities because is impossible to eliminate all vulnerabilities*".

Factor 8: Reassured by statements on the website related to sharing but retained their scepticism:

Factor 8 has 2 significantly loading participants (2M/0F) with an average age of 26.5 years. It explains 4% of the variance.

These participants wanted as much information as possible "*I feel that people should be fully informed when it comes to how their data is used/shared. Therefore; the more informed I am, I can make a confident informed decision to share my information.*"

Even so, they did not abandon their intuitive scepticism. For example, one participant said, in responding to the statement that the website is monitored 24/7: "*This seems also so illogical and hard to believe, which makes the website look bad in my eyes.*". They also did not trust customer reviews: "*Most of the times they are written by the owner of the website. They represent mistrust in me.*"

4.4. Returning to the research question

It is clear, from this study, that people want reassurance that the website takes their data custodianship role seriously.

5. Study 3 - CyberDiary

Humans are at the heart of all cybersecurity processes, and all of us are driven by our emotions. As the famous author Haidt described in his book "The Happiness Hypothesis" (Haidt, 2006), the human brain is like a man on an elephant; the elephant represents our emotions, whereas the man represents our rational side. Researchers have been focusing so far on the man who sits on top of the elephant. Here, we investigate the nature of the elephant in the context of cybersecurity. Studies in this area have shown that most emotions related to cybersecurity tend to be negative (Renaud et al., 2021), but confirmation of these findings would be useful.

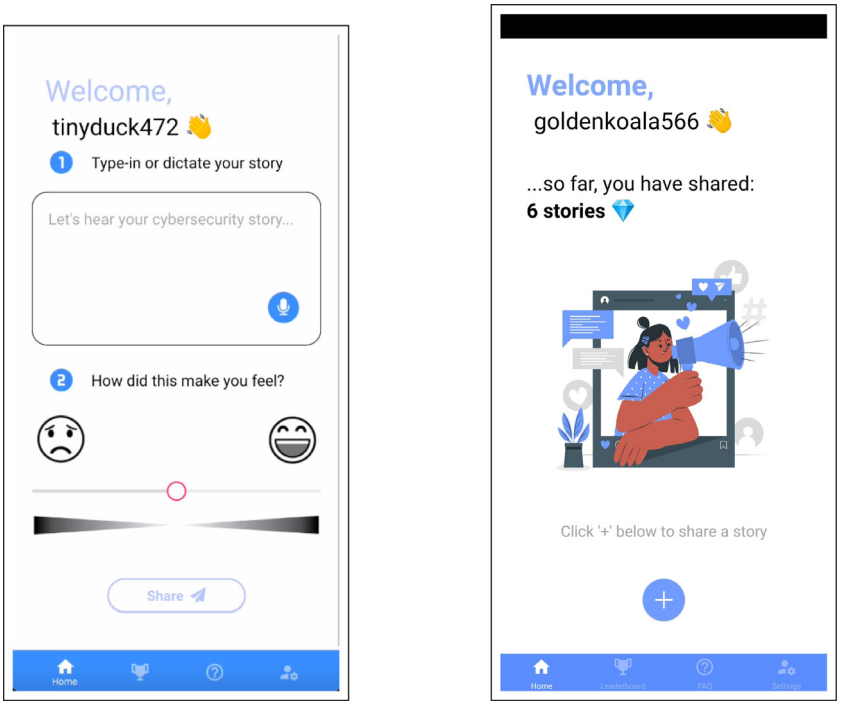

Fig. 12. Home screen: Before and after user testing.

We carried out a study where we simply asked participants for their cybersecurity stories without any framing — so as to ensure that we did not prime responses, either negatively or positively. This section reports on this final study to answer the final research question (RQ3): "*How do people feel about cybersecurity generally?*"

CyberDiary is a mobile application which facilitated the sharing of cybersecurity stories anonymously. When sharing a story, users were asked to attribute an emotion, depicting how they felt in relation to the story.

5.1. Implementation

CyberDiary was implemented using React Native. The stories were stored anonymously, on Firebase, which is certified under major privacy and security standards.[6] The study received ethical approval from the University of [Redacted].

Accessible Story Entry: To ease story entry, we allowed participants to type their story, or record the story in audio. Blue was used as the main colour and orange as the secondary colour, to ensure that colour-blind users would not experience difficulties using it. The app used sans-serif fonts to accommodate those with dyslexia. CyberDiary used emojis, illustrations and icons to accommodate those with low literacy. The interface was simplified as much as possible based on pilot tests, minimising the steps involved in sharing a cyber story (see Fig. 12).

Encouraging Stories: To encourage participants to tell us their stories, we relied on the literature on habit (Duhigg, 2013). Duhigg introduces the 'habit loop', which essentially refers to the cyclical relationship between a cue, routine (action) and reward. According to Duhigg, to make a habit persist, these three elements need to be carefully chosen and designed. The cue was provided by CyberDiary notifications (with time and frequency being chosen by the participant). The reward is shown in Fig. 13.

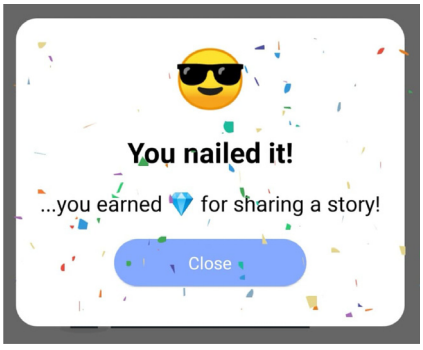

Fig. 13. Rewarding participants for stories.

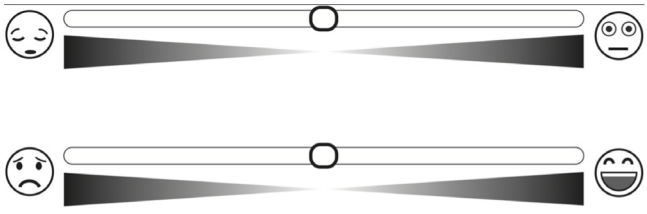

Fig. 14. AS — the Affective Slider (Betella, 2016).

Measuring Emotion: The "Affective Slider" (see Fig. 14) was developed and tested by Betella (2016). This solution measures emotions and consists of two slider controls which measure emotions in terms of pleasure and arousal. For the purposes of this study, we only focus on capturing the levels of pleasure.

5.2. Gathering stories

29 participants were recruited using snowball sampling. Recruited users had different levels of experience with technology

[6] Google. Privacy and Security in Firebase. https://firebase.google.com/support/privacy(visitedon03/09/2022).

and were natively from various countries (Romania, Bulgaria, Greece, the UK). Their ages ranged from 18 to 76.

Participants were asked to use the app for a period of 4 weeks. Participants registered to use CyberDiary, and provided a total of N = 86 stories.

Overall, the mobile application produced was found to be very easy to use ("Straightforward to use."), intuitive ("Nice colours and design") and user-friendly ("Welcoming, friendly interface. Easy usability."), achieving an average usability score of 91.25, based on the System Usability Survey[7] score.

5.3. Analysis

Using a well-known online sentiment analysis tool, MonkeyLearn (2022), we aimed to re-evaluate the emotions attached to the stories to determine whether users' own expressed emotions match the emotion reported by the sentiment analysis tool. In 22 cases, the emotions reported by the sentiment analysis tool did not match the ones users reported. Since the tool is based on an AI which is far from perfect, it was decided that the best course of action was to manually go through these stories and determine the most probable emotion. In most cases, users' own assessment was the one taken into consideration for the final analysis.

Overall, across all participants, a clear tendency towards negative emotions in relation to cybersecurity was discovered. Negative experiences outweigh the positive ones by 20%. This widespread negativity is further analysed in the context of users' responses. The biggest difference between positive and negative experiences was seen in the people aged between 57 and 76 (Baby Boomers), 85% relating negative experiences.

One possible explanation for the widespread negativity across all generations could be the psychological principle that bad experiences have more impact on people than good ones (Baumeister et al., 2001). As a consequence, they become more memorable. This is said to have had an evolutionary importance, allowing humans to know what and whom to avoid in order to escape danger. In our case, this means that when asked to look back to relate their cybersecurity stories, people would most likely connect to previous experiences that affected them negatively, seeing narration as a way of alleviating their pain or a way to help others avoid the same experiences.

To gather more in-depth insights about the topics raised by users, the stories were also put through a text analysis tool (Voyant Tools Tools, 2022). It was discovered that most stories were related to 'email', 'account', 'internet', 'website', 'phone', 'card' and 'authentication'. Example stories based on the associated reaction:

Positive: *"Everyday looking on my BitDefender, if it is running, if I am 'protected', my checking is a sort of self-care. As when I check the door lock in the night going to bed."* (R56)

Negative: *"You always hear stories about hackers stealing data from various companies or stealing millions from crypto exchanges or shutting down nuclear facilities. How safe are we if billion dollar companies cannot protect themselves against hackers?"* (R45)

Neutral: *"Back in summer 2017, I managed to host an almost perfect clone for Facebook website and shared the URL on my newsfeed to see how many people would fall for this trap, sending me their credentials. I got about 6 passwords in 30 min. Don't know whether to laugh or cry."* (R36)

5.4. Returning to the research question

Similar to Renaud et al. (2021), we found that people predominantly expressed negative emotions towards cybersecurity, even when health data is not mentioned.

[7] https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html.

6. Discussion & reflection

The first research question was: "*RQ1: Will a metaphor be effective in helping people to understand how encryption works?*" Our rationale was that if people understood the underlying protective mechanisms, this would be likely to engender trust, and increase the prevalence of data sharing. Study 1 (Section 3) revealed that our 217 participants did not want this level of technical knowledge: they wanted to be able to gauge the trustworthiness of the online service based on explicit reassurances provided by the service provider. Hence, the answer to RQ1 is: "understanding is not what users need", they need reassurance.

The second study investigated the following research question: "*RQ2: What cues do people rely on in making privacy-related decisions?*" We fed open text responses from the first study into statements related to three particular kinds of "choice architecture" elements mentioned above i.e., cues that could activate heuristics in decision making contexts. Our second study (Section 4) used these statements in a Q-sort to assess the extent to which people agreed with these in the health data sharing context. The second study revealed that people want to see cues attesting to the organisation's efforts, and measures implemented, to protect their personal information. They want reassurance before they divulge their information. They are looking for compelling reasons to be reassured that the online service is making an effort to secure their personal information. If online services do not provide such reassurance, the underlying scepticism might well cause users to abandon the service.

The first two studies were carried out in the specific context of heath information and the scepticism in this context is undoubtedly negative. The third study (Section 5) was carried out to ascertain whether this negativity was specific to the health information sharing context, or whether it infused cybersecurity more generally, as suggested by Renaud et al. (2021). To confirm this, we asked people to share their cyber stories, with no framing or implied context to answer the third research question: "*RQ3: How do people feel about cybersecurity generally?*" This final study, with 29 participants, revealed the same negativity infusing the wider cybersecurity context. The stories participants told us were unprompted and not framed in any way. Hence, the negativity can be argued to have originated from participants' personal experiences. Hence the answer to RQ3 is: 'many experience it negatively'.

Research & practical implications

The *research* implications of this are twofold. The first are related to the privacy paradox. It might well apply in some contexts but its influence is likely to be more nuanced and uncertain in others. Certainly, more research needs to be undertaken into the applicability of the privacy paradox in a variety of contexts. The second are related to investigating how we ought to accommodate the negativity many feel towards cybersecurity. Unless we do this, awareness and training efforts are likely to be less effective than they could be.

In *practical* terms, we should assume that users **do** care and act accordingly. Those who collect people's information online should make a deliberate effort to implement measures to secure this information *and explicitly mention these on the site when asking for that information*. People want reassurance to help them to make decisions about the trustworthiness of data custodians. Online services should not neglect to provide this because people do indeed rely on visible cues to make these decisions.

Table A.2
P-values for post-hoc tests for perceived usefulness of different information types.

	Ethical hackers	Anonymisation	Compliance	Security standards
Anonymisation	0.30			
Compliance	0.50	*0.00		
Security standards	1.00	0.25	0.57	
Cryptography	0.55	0.99	*0.02	0.48

*Signifies statistical significance.

Table A.3
P-values for post-hoc tests for perceived usefulness of different information types.

	Expert endorsement	Compliance	Storage of collected data	App developers	Collected data	Data shared with third parties	Reviews from other users
Compliance	*0.02						
Storage of collected data	0.16	1.00					
App developers	0.44	*0.00	*0.00				
Collected data	*0.00	0.30	0.05	*0.00			
Data shared with third parties	*0.00	*0.00	*0.00	*0.00	0.32		
Reviews from other users	1.00	*0.03	0.23	0.34	*0.00	*0.00	
Technical details	0.27	*0.00	*0.00	1.00	*0.00	*0.00	0.20

*Signifies statistical significance.

Limitations

Unintended side effects: In carrying out this research, we do not aim to give bad agents a range of deception strategies to use in order to encourage unwise disclosures. We abhor these kinds of 'dark patterns' (Waldman, 2020). Our aim was to understand how people were making decisions and to reveal subjective thinking in this respect.

Sampling bias: We used a crowd-sourcing platform for our studies. While this method for sampling the participants is widely accepted in empirical research, it has certain limitations. In particular, one of them is that the users of such platforms tend to be younger and more educated than the general population, as well as more actively using the Internet (Redmiles et al., 2019). Our results might therefore be representative of particular demographics. Further studies are needed to understand attitudes towards privacy assurances among older or less educated population. In particular, our participants are very young (most are in their 20s). This means that we do not know how our findings will generalise to older populations. On the other hand, these findings go against the common narrative of "*young people don't care about privacy*" (Malcolm, 2021), confirming the conclusions of Hoofnagle et al. (2010), Richards (2015), Blank et al. (2014) and Stanley (2013). Van Der Velden and El Emam (2013) found the same privacy protective behaviour related to disclosure of health information. These findings, and ours, suggest that young people are likely to be as least as privacy conscious as their elders.

Self-reporting: While our participants claim that they want to read additional information and exercise control over their data, these aspirations might not necessarily translate to practice, especially given the number of digital services people interact with on a daily basis. In particular, participants mentioning the importance of assurances to them (see e.g. Section 3.4.2) might be influenced by the overall framing of the study. Our findings nonetheless show that users are interested in regaining control over their data. The fact that they often make decisions that negatively affect their privacy, however, might point to the inadequacy of currently displayed cues. This chimes with previous research saying that it is the "self management of privacy" model that is deficient, not people's desire to protect their own privacy (Solove, 2013). A structural approach is required to address these deficiencies (Seberger et al., 2021).

Sample Size: The third study had only 29 participants. It would be worth repeating this study with a larger number of participants.

7. Conclusion

Our three studies revealed scepticism and general negativity towards cybersecurity. Even so, people were willing to process additional information in form of security and privacy reassurances. These could be commitments to legal standards such as GDPR or evidence that the site has been tested by a security professional. Online service users definitely wanted more control over their personal information, and they were willing to read security-related information provided by service providers.

Our findings conclude that, despite seeming apathetic towards their personal privacy, data subjects do indeed want to be involved in decisions regarding their personal information. Hence, improved mechanisms for providing verified reassurances will prove beneficial to both users and service providers. Service providers need to acknowledge the underlying scepticism and act to relieve it — otherwise some might decline to use the service due to their unalleviated concerns.

In conclusion, assuming that people do not care about their privacy, and then using that assumption to justify not providing meaningful cues to users, is an ill-advised strategy. It does not engender trust from users who will only divulge information if they are sufficiently reassured by the choice architecture features, including cues. Acknowledging this fact is part of a bigger lesson that comes from this study: emotions are important and negative emotions are damaging. This fact needs to be acknowledged and accommodated in our designs of security and privacy systems.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Appendix

See Fig. A.15 and Tables A.2–A.4.

Table A.4
Final Q-Statements (Statements in Quotes) (Subscripts refer to classification in terms of Fig. 1).

1. "Your information is stored in a GDPR compliant way[b]"	20. Assurances only serve to worry me[a]
2. "Privacy International has accredited our website[b]"	21. My friends recommended this website to me[a]
3. "This website is WCAG compliant[b]"	22. If I see any assurance, I feel more protected[a]
4. "We will not sell or share your information with anyone[b]"	23. It depends on the kind of information that I am asked to share[a]
5. "Ethical hackers have tested this website and certified its security[b]"	24. "Vulnerabilities have been identified and eliminated"[b]
6. "We give you fine-grained controls over which of your data to share[b]"	25. I don't trust any assurances about encryption[a]
7. "For better security, you can activate two-factor authentication[b]"	26. I would never share my personal information regardless of assurances[a]
8. "Our reputation depends on us not violating your trust[b]"	27. Statements from well known security experts praising the website for good practice[a]
9. "Your information is encrypted using the Advanced Encryption Standard (AES)[b]"	28. The number of website customers who have ranked the website positively[a]
10. "We are ISO 27 001 compliant[b]"	29. The more information that is provided, the more I likely would I would be trust them[a]
11. "We have industry standard measures in place to secure your information[b]"	30. "If they ask for my consent, I would be more likely to trust them[a]"
12. "The website looks professional[c]"	31. "I don't want too much security information[a]"
13. "We have never experienced an information breach"[b]	32. Life is too short to read all this information[a]
14. "We have an in-house security team monitoring our website 24/7[b]"	33. "I have nothing to hide[a]"
15. "We have repelled over 1000 cyber attacks in the last year[b]"	34. I don't trust anonymisation[a]
16. "It doesn't matter what I see. I will use it[a]"	35. "We anonymise all your information[b]"
17. "I just have to trust any website because I don't understand security[a]"	36. "We do not collect any non-essential information, only what we need to fulfill your order[b]"
18."The website's language is simple and easy to understand[c]"	37. "Your information will be deleted as soon as the legally required retention period is over[b]"
19. "The assurances have clearly been written by a lawyer[c]"	38. "The website provides a link to extensive information about security and privacy[c]"

[a]Individual rationalisations.
[b]Reassurance statements.
[c]Observations based on website features.

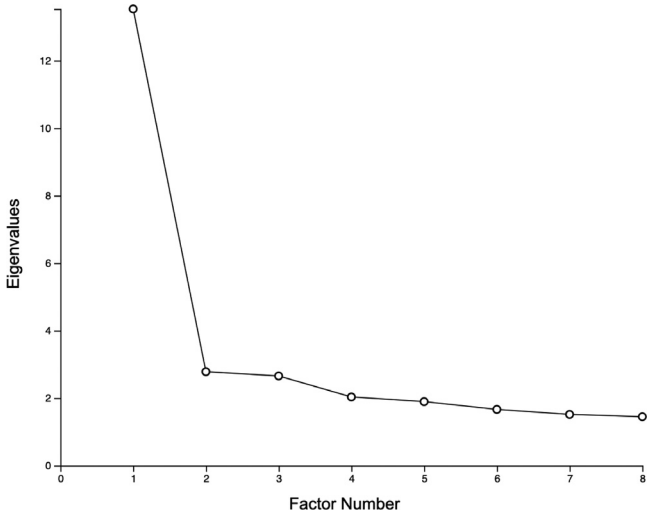

Fig. A.15. Scree plot.

References

Acquisti, A., Gritzalis, S., Lambrinoudakis, C., di Vimercati, S., 2007. What Can Behavioral Economics Teach us about Privacy?. Auerbach Publications.

Agresti, A., 2003. Categorical Data Analysis. John Wiley & Sons.

Aïmeur, E., Lawani, O., Dalkir, K., 2016. When changing the look of privacy policies affects user trust: An experimental study. Comput. Hum. Behav. 58, 368–379.

Allidina, S., Cunningham, W.A., 2021. Avoidance begets avoidance: A computational account of negative stereotype persistence. J. Exp. Psychol. [Gen.] 150 (10), 2078–2099. http://dx.doi.org/10.1037/xge0001037.

Barth, S., de Jong, M.D., Junger, M., Hartel, P.H., Roppelt, J.C., 2019. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. Telemat. Inform. 41, 55–69.

Baumeister, R.F., Bratslavsky, E., Finkenauer, C., Vohs, K.D., 2001. Bad is stronger than good. Rev. Gen. Psychol. 5 (4), 323–370.

Becker, M., Matt, C., Hess, T., 2020. It's Not Just About the Product: How Persuasive Communication Affects the Disclosure of Personal Health Information. ACM SIGMIS Database: DATABASE Adv. Inf. Syst. 51 (1), 37–50.

Bekker, H., Thornton, J., Airey, C., Connelly, J., Hewison, J., Robinson, M., Lilleyman, J., MacIntosh, M., Maule, A., Michie, S., Pearman, A., 1999. Informed decision making: an annotated bibliography and systematic review. Health Technol. Assess. 3 (1), 1–156.

Beldad, A., van der Geest, T., de Jong, M., Steehouder, M., 2012. Shall I tell you where I live and who I am? Factors influencing the behavioral intention to disclose personal data for online government transactions. Int. J. Human-Comput. Interact. 28 (3), 163–177.

Benjamini, Y., Hochberg, Y., 1995. Controlling the false discovery rate: a practical and powerful approach to multiple testing. J. R. Stat. Soc. Ser. B Stat. Methodol. 57 (1), 289–300.

Betella, P.F.M.J., 2016. The affective slider: A digital self-assessment scale for the measurement of human emotions. PLOS ONE 11 (2), 1–11. http://dx.doi.org/10.1371/journal.pone.0148037.

Betz, D.J., Stevens, T., 2013. Analogical reasoning and cyber security. Secur. Dialogue 44 (2), 147–164.

Betzing, J.H., Tietz, M., vom Brocke, J., Becker, J., 2020. The impact of transparency on mobile privacy decision making. Electron. Mark. 30 (3), 607–625.

Bhuiyan, M.M., Whitley, H., Horning, M., Lee, S.W., Mitra, T., 2021. Designing transparency cues in online news platforms to promote trust: Journalists & consumers perspectives. Proc. ACM Human-Comput. Interact. 5 (CSCW2), 1–31.

Blank, G., Bolsover, G., Dubois, E., 2014. A new privacy paradox: Young people and privacy on social network sites. In: Prepared for the Annual Meeting of the American Sociological Association, Vol. 17.

Branch, J., 2021. What's in a name? Metaphors and cybersecurity. Int. Organ. 75 (1), 39–70.
Brown, S.R., 1993. A primer on q methodology. Operant Subj. 16 (3/4), 91–138. http://dx.doi.org/10.15133/j.os.1993.002.
Canbek, G., 2018. Cyber security by a new analogy: "The allegory of the mobile cave". J. Appl. Secur. Res. 13 (1), 63–88.
Chambers, J.M., Freeny, A.E., Heiberger, R.M., 2017. Analysis of variance; designed experiments. In: Statistical Models in S. Routledge, pp. 145–193.
Coles-Kemp, L., Kani-Zabihi, E., 2010. On-line privacy and consent: a dialogue, not a monologue. In: Proceedings of the 2010 New Security Paradigms Workshop. pp. 95–106.
Dechand, S., Naiakshina, A., Danilova, A., Smith, M., 2019. In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception. In: 2019 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, pp. 401–415.
Demjaha, A., Spring, J.M., Becker, I., Parkin, S., Sasse, M.A., 2018. Metaphors considered harmful? An exploratory study of the effectiveness of functional metaphors for end-to-end encryption. In: Proc. USEC, Vol. 2018. Internet Society.
Dienlin, T., Trepte, S., 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. Eur. J. Soc. Psychol. 45 (3), 285–297.
Diggelmann, O., Cleis, M.N., 2014. How the right to privacy became a human right. Human Rights Law Rev. 14 (3), 441–458.
Duhigg, C., 2013. The Power of Habit. Random House Books, London.
Equality and Human Rights Commission, 2021. Article 8: Respect for your private and family life. Retrieved 19 June from: https://www.equalityhumanrights.com/en/human-rights-act/article-8-respect-your-private-and-family-life.
Gruzd, A., Hernández-García, Á., 2018. Privacy concerns and self-disclosure in private and public uses of social media. Cyberpsychol. Behav. Soc. Netw. 21 (7), 418–428.
Haidt, J., 2006. The Happiness Hypothesis. Basic Books, New York, pp. 11–16.
Hollander, M., Wolfe, D.A., 1973. Nonparametric Statistical Methods. John Wiley & Sons.
Hong, W., Chan, F.K., Thong, J.Y., 2019. Drivers and inhibitors of internet privacy concern: a multidimensional development theory perspective. J. Bus. Ethics 168, 539–564.
Hoofnagle, C.J., King, J., Li, S., Turow, J., 2010. How different are young adults from older adults when it comes to information privacy attitudes and policies? Available at SSRN 1589864.
Jensen, C., Potts, C., 2004. Privacy policies as decision-making tools: an evaluation of online privacy notices. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 471–478.
Jozani, M., Ayaburi, E., Ko, M., Choo, K.-K.R., 2020. Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. Comput. Hum. Behav. 107, 106260.
Kahneman, D., 2011. Thinking, Fast and Slow. Macmillan.
Karas, T.H., Moore, J.H., Parrott, L.K., 2008. Metaphors for Cyber Security. Sandia Report SAND2008-5381, Sandia Labs, NM.
Kehr, F., Kowatsch, T., Wentzel, D., Fleisch, E., 2015. Thinking styles and privacy decisions: need for cognition, faith into intuition, and the privacy calculus. In: 12th International Conference on Wirtschaftsinformatik (WI 2015). Universität Osnabrück.
Kim, M.S., Kim, S., 2018. Factors influencing willingness to provide personal information for personalized recommendations. Comput. Hum. Behav. 88, 143–152.
Kokolakis, S., 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Comput. Secur. 64, 122–134.
Kulyk, O., Milanovic, K., Pitt, J., 2020. Does my smart device provider care about my privacy? Investigating trust factors and user attitudes in IoT systems. In: Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society. pp. 1–12.
Lapointe, A., 2011. When Good Metaphors Go Bad: The Metaphoric "Branding" of Cyberspace, Vol. 9. Center for Strategic and International Studies, https://ciaotest.cc.columbia.edu/wps/csis/0023199/f_0023199_18988.pdf.
Lawson, S., 2012. Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. First Monday 17 (7), http://dx.doi.org/10.5210/fm.v17i7.3848.
Li, H., Luo, X.R., Zhang, J., Xu, H., 2017. Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. Inf. Manag. 54 (8), 1012–1022.
Maio, G.R., Esses, V.M., 2001. The need for affect: Individual differences in the motivation to approach or avoid emotions. J. Personal. 69 (4), 583–614.
Malcolm, H., 2021. Millennials don't worry about online privacy. https://eu.usatoday.com/story/money/business/2013/04/21/millennials-personal-info-online/2087989/.
Martin, L.L., Ward, D.W., Achee, J.W., Wyer, R.S., 1993. Mood as input: People have to interpret the motivational implications of their moods. J. Personal. Soc. Psychol. 64 (3), 317–326.
Mazurek, G., Małagocka, K., 2019. What if you ask and they say yes? Consumers' willingness to disclose personal data is stronger than you think. Bus. Horiz. 62 (6), 751–759.
McHugh, M.L., 2012. Interrater reliability: the kappa statistic. Biochem. Med. 22 (3), 276–282.
MonkeyLearn, 2022. Sentiment analyzer. URL https://monkeylearn.com/sentiment-analysis-online/.
Morgan, S.E., Reichert, T., 1999. The message is in the metaphor: Assessing the comprehension of metaphors in advertisements. J. Advert. 28 (4), 1–12.
Nemenyi, P.B., 1963. Distribution-Free Multiple Comparisons. Princeton University.
Olausson, M., 2018. User Control of Personal Data: A Study of Personal Data Management in a GDPR-Compliant Grahpical User Interface (Thesis). Linnaeus University, Faculty of Technology, Department of Computer Science and Media Technology.
Raja, F., Hawkey, K., Hsu, S., Wang, K.-L.C., Beznosov, K., 2011. A brick wall, a locked door, and a bandit: a physical security metaphor for firewall warnings. In: Proceedings of the Seventh Symposium on Usable Privacy and Security. pp. 1–20.
Redmiles, E.M., Kross, S., Mazurek, M.L., 2019. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In: IEEE Symposium on Security and Privacy. SP, IEEE, pp. 1326–1343.
Renaud, K., Zimmermann, V., Schürmann, T., Böhm, C., 2021. Exploring cybersecurity-related emotions and finding that they are challenging to measure. Humanit. Soc. Sci. Commun. 8, 1–17. http://dx.doi.org/10.1057/s41599-021-00746-5, 2021 8:1.
Richards, N.M., 2015. Four Privacy Myths. Revised form, A World Without Privacy. Cambridge Press, Austin Sarat, forthcoming, Available at SSRN: https://ssrn.com/abstract=2427808.
Schaap, B., Anand, S., Laperrière, A., 2020. Improving data access for more effective decision making in agriculture. In: Improving Data Management and Decision Support Systems in Agriculture. Burleigh Dodds Science Publishing, pp. 3–16.
Scott, P., Vlimki, M., Leino-Kilpi, H., Dassen, T., Gasull, M., Lemonidou, C., Arndt, M., 2003. Autonomy, privacy and informed consent 1: concepts and definitions. Br. J. Nurs. 12 (1), 43–47.
Seberger, J.S., Llavore, M., Wyant, N.N., Shklovski, I., Patil, S., 2021. Empowering resignation: There's an app for that. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. pp. 1–18.
Shouse, E., 2005. Feeling, emotion, affect. M/C J. 8 (6), http://dx.doi.org/10.5204/mcj.2443.
Skrynnikova, I., 2020. Metaphor Co-Creation in Reframing Cybersecurity Issues. Rev. Electrón. Lingüíst. Apl. 19 (1), 58–77.
Solove, D.J., 2013. Privacy self-management and the consent dilemma. Harv. Law Rev. 126, 1880–1903.
Solove, D.J., 2020. The myth of the privacy paradox. George Wash. Law Rev. 89, 1–46.
Stanley, H., 2013. Do young people care about privacy?. https://www.aclu.org/blog/privacy-technology/consumer-privacy/do-young-people-care-about-privacy.
Stephenson, W., 1935. Correlating persons instead of tests. J. Personal. 4 (1), 17–24. http://dx.doi.org/10.1111/j.1467-6494.1935.tb02022.x.
Sundar, S.S., Kim, J., Rosson, M.B., Molina, M.D., 2020. Online privacy heuristics that predict information disclosure. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. pp. 1–12.
Sunstein, C.R., Thaler, R.H., 2014. Nudge: Improving Decisions About Health, Wealth, and Happiness. Penguin Books.
Taylor, C., Dewsbury, B.M., 2018. On the problem and promise of metaphor use in science and science communication. J. Microbiol. Biol. Educ. 19 (1), 2.
Thibodeau, P., Durgin, F.H., 2008. Productive figurative communication: Conventional metaphors facilitate the comprehension of related novel metaphors. J. Memory Lang. 58 (2), 521–540.
Thibodeau, P.H., Matlock, T., Flusberg, S.J., 2019. The role of metaphor in communication and thought. Lang. Linguist. Compass 13 (5), e12327.
Tools, V., 2022. See through your text. URL https://voyant-tools.org/.
Trepagnier, P., 2019. Cyber metaphors and cyber goals: Lessons from "Flatland". Mil. Cyber Aff. 4 (1), 2. http://dx.doi.org/10.5038/2378-0789.4.1.1045.
Van Der Velden, M., El Emam, K., 2013. "Not all my friends need to know": a qualitative study of teenage patients, privacy, and social media. J. Am. Med. Inform. Assoc. 20 (1), 16–24.
Waldman, A.E., 2020. Cognitive biases, dark patterns, and the 'privacy paradox'. Curr. Opin. Psychol. 31, 105–109.
Wang, Y.D., Emurian, H.H., 2005. Trust in e-commerce: consideration of interface design factors. J. Electron. Commer. Organ. (JECO) 3 (4), 42–60.
Ward, D., 2010. It's Not a Big Truck: Examining Cyber Metaphors. Tech. rep., Office of the Deputy Assistant Secretary of the Air Force for Acquisition, https://apps.dtic.mil/sti/citations/AD1016349.

Wästlund, E., Angulo, J., Fischer-Hübner, S., 2011. Evoking comprehensive mental models of anonymous credentials. In: International Workshop on Open Problems in Network Security. Springer, pp. 1–14.

Watts, S., Stenner, P., 2005. Doing Q methodology: theory, method and interpretation. Qual. Res. Psychol. 2 (1), 67–91. http://dx.doi.org/10.1191/1478088705qp022oa.

Westin, A.F., 2003. Social and political dimensions of privacy. J. Soc. Issues 59 (2), 431–453.

Xie, E., Teo, H.-H., Wan, W., 2006. Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. Mark. Lett. 17 (1), 61–74.