"*I need to know I'm safe and protected and will check*": Users Want Cues to Signal Data Custodians' Trustworthiness

Oksana Kulyk
University of Copenhagen, Denmark
Karlsruhe Institute of Technology, Germany
Email: okku@itu.dk

Karen Renaud
University of Strathclyde, UK
Rhodes University, South Africa
University of South Africa, South Africa
Email: karen.renaud@strath.ac.uk

***Abstract*—Privacy-related decisions are complex and nuanced, and consume extensive cognitive resources. Yet, people make these kinds of decisions many times a day. This means that they might not be able to invest significant cognitive resources in making each and every decision. We tested the extent to which the statements displayed to the users with the purpose of assuring them that their security and privacy is protected would resonate with people when they were considering whether or not to divulge their personal health information to an online service. We carried out two empirical investigations: (1) we used scenarios of health data being transmitted securely to a health provider, and asked participants to tell us what would convince them to divulge their personal information. (2) We then used these statements in a Q-sort to gauge subjective opinions of the persuasiveness of the statements, and to reveal 'ways of thinking' engaged in by our participants in this respect. We discovered that our participants wanted to see evidence that the organisation was implementing required security measures. Thus, our study suggests, despite a common assumption, that people do care, and that they want reassurance that companies are trustworthy custodians of their health data.**

I. Introduction

Privacy is a fundamental human right [1], which came into existence after the second World War [2]. 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 [3], others have studied the influence of thinking styles on privacy decisions [4], and yet others consider how to encourage people to read privacy policies [5].

Privacy decisions are complex and cognitively demanding [6], [7]. Hence, it seems that people will consider particular cues in helping them to make privacy-related decisions. Provision of extra information might also exacerbate complexity [8], so it is important to consider what kind of choice architecture cues would help people make informed privacy-protective decisions, without increasing cognitive load.

The privacy paradox theory suggests that people's self-reported intentions to act to preserve their own privacy do not convert to action [9]. Some researchers have carried out studies that seem to confirm the existence of the paradox [10]–[12]. Yet, a number of other researchers argue that the paradox is an artefact of the way the experiments are carried out [13]–[16]. 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. This mismatch might lead to the conclusion that people do not really value their privacy. Our research question is thus: "*What kinds of choice architecture cues would convince people to trust online services with their health data, or do they simply not care about privacy?*"

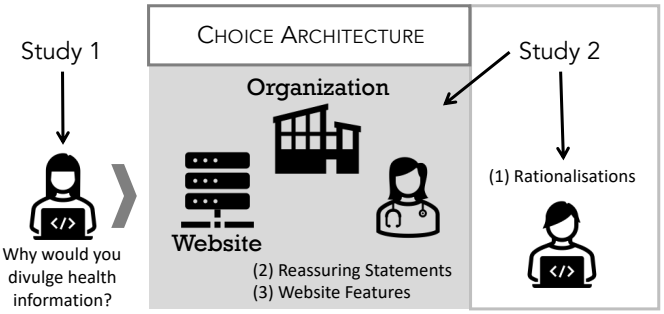

Fig. 1. Decision Influences

As shown in Figure 1, we commenced by carrying out a preliminary study to assess what people said about divulging their personal data to an online health service (this ensured that the statements they made were informed by the context we sketched. We used their responses to derive three particular kinds of "choice architecture" elements [17]: *first*, number 1 in the diagram points to the individual perceptions of the decision maker him or herself. For example, if a person avoids making cyber security related decisions, he or she might decide to trust all or no websites, regardless of anything the website interface displays. *Second*, number 2 in the diagram points to particular statements on the website that might serve to reassure the user. *Third*, number 3 on the diagram is related to the look and feel of the website itself. The second and third aspects are context-dependent while the first is more related to the individual and their experiences and general attitudes, irrespective of the website being used.

Both of our studies were empirical, implemented as online surveys with 217 and 40 participants respectively. The first study followed a qualitative approach in form of open-ended questions. The main study relied on Q-methodology, a mixed-methods approach designed specifically to study subjectivity.

We found that participants wanted additional information in form of security and privacy assurances (such as, for example, commitment to legal standards such as GDPR). They 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 apathy related to personal privacy, data subjects do indeed want to be involved in decisions regarding their personal information. Hence, improved mechanisms for providing verified reassurances should be developed.

In Section II we commence by reviewing the related research. Section III describes Study 1, reporting the materials, methodology, and results of the study. Section IV then presents Study 2, which tested context and non-context sensitive influences on privacy decisions. Section V discusses and reflects on our findings.

II. Related Research

We describe findings from previous research on using metaphors in cybersecurty as well as investigating factors influencing online information disclosure.

Mazurek and Małagocka [18] 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. Such trust reduces uncertainty, perceived risk and randomness and its importance confirmed by many researchers [19]–[21].

Robinson [22] finds that the decision to disclose personal information depends on the perceived benefits that can be obtained if such details are divulged. The same internal cost-benefit calculus being engaged in when considering whether to disclose or not is also reported by [21], [23]. There is evidence that people do indeed seriously consider the risks of disclosure, especially when health information is involved [24].

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 [20], [25], [26].

III. Study 1 - Privacy Decision Rationalisations

Research Question: *How do people rationalise their decisions to divulge their health data to an online service?*

The **outcome** of this study was statements to feed into the second study to assess subjective opinions.

A. Materials

The first study presents a scenario of a health tracker app that provides the option either to share their health data with their healthcare provider, or to keep it locally on the user's smartphone. The users are shown this choice using a metaphor to highlight protection afforded by encryption during transmission of their data to a trusted healthcare provider. We selected three metaphors and assigned participants randomly to one of them: *(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. *(2) Language* presenting encrypted data as being translated into a secret unique language, with only authorised entities being able to understand it. *(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 eavesdrop.

B. Study procedure

The study was a between-subjects online survey, with participants being recruited via the Prolific platform[1]. The participants were paid £1.25 for estimated 10 minutes of labour, exceeding the UK minimum wage.

Before starting the study, the participants were presented with a consent form, outlining the purpose of the study and assuring them that their responses would be anonymous. They were then presented with a description of a potential health tracker app, presented with a visual representation of a corresponding metaphor (randomly assigned to the participant). The participants were then asked a number of questions regarding their willingness to share the data and their understanding of the level of security the app provides (based on the description they received)[2]

Afterwards, participants were asked whether they would like to see additional information before they decided whether to upload their data. They were then presented with the list of each type of information (e.g. "*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*" and asked to rate how useful they would find each type of information (5-point Likert scale, from "not useful at all" to "very useful").

The study concluded with questions about demographics.

C. 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.

[1]https://www.prolific.co/

[2]For the sake of brevity, we omit our evaluation of these questions from the paper, and provide it in the extended version of the paper.

1) Usefulness of provided information: Overall, 51% of participants answered that they were either "rather likely" or "very likely" to share data. Nonetheless, 85% of the participants responded that they would want to see additional information before deciding on data disclosure. When asked to rate specific types of information, in terms of usefulness, the top rated types 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 developers" 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).

2) Assurances: The majority of the participants found that assurances make it more likely for them to disclose their data (rating them as "slightly more likely", "more likely" or "much more likely"). Others felt that the assurances would not change the likelihood of sharing data, as compared to the previously shown notice. An overview of ratings is provided on Figure 3. There is a significant difference between the assurances (Friedman test, $\chi^2(4, N = 217) = 22.411$, $p < .001$, effect size $W = .0258$, small)[3]. The assurances rated most likely to lead to data sharing were "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 "much less likely", "less likely", "slightly less likely" by 30%, 20%, 13% of participants respectively).

D. Deriving the Q-Statements

The outcome of this study feeds into the second study. We thus needed to derive Q-statements for that purpose. We decided to rely on the free-text responses provided by the participants, given that these reflected *their* perceptions about what would encourage them to divulge their information within a particular context.

We worked independently through the comments provided by the participants 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. The authors worked through the list together to combine semantically similar statements that we could use to confirm public perceptions of the persuasiveness of the different reassuring statements. The final statements are shown in Table III in Appendix A.

The statements reflect a mixture of influences (see Figure 1): (1) individual rationalizations (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 III.

IV. Study 2 - Trustworthiness Cues

We investigated the following **research question**:

> *How do people reason about divulging their health data, based on the statements they see on a website accompanying requests for their data?*

A. 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 [27] to gauge this. It supports a systematic study of subjectivity. Q-methodology is an informal instantiation of Cultural Consensus Theory [28], providing a framework for the measurement of beliefs *as cultural phenomena*. It supports researchers in revealing beliefs shared by groups of individuals. The findings from a Q-methodology reveal the *nature* of subjectivity. It reveals '*what is the nature of different groups' thinking?*', not '*how are people thinking on the topic?*'. This methodology considers large numbers of participants to be '*relatively unimportant*' [29].

The method reveals correlations between subjects across a sample of variables, referred to as the "Q set", which 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, and supports a qualitative analysis. In addition to asking people to sort statements, it also requests free text responses where people can explain why they ranked different statements on either the right or the left (disagree vs. agree). It is not designed to prove or disprove hypotheses, but to provide a sense of '*potentially complex and socially contested*' issues [30]. Figure 4 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 agreeable (ranked +3) and most disagreeable (ranked -3) statements. This serves to gain '*an impression of the range of opinion at issue*' [29].

[3]The post-hoc tests describing differences between assurances are provided the Appendix

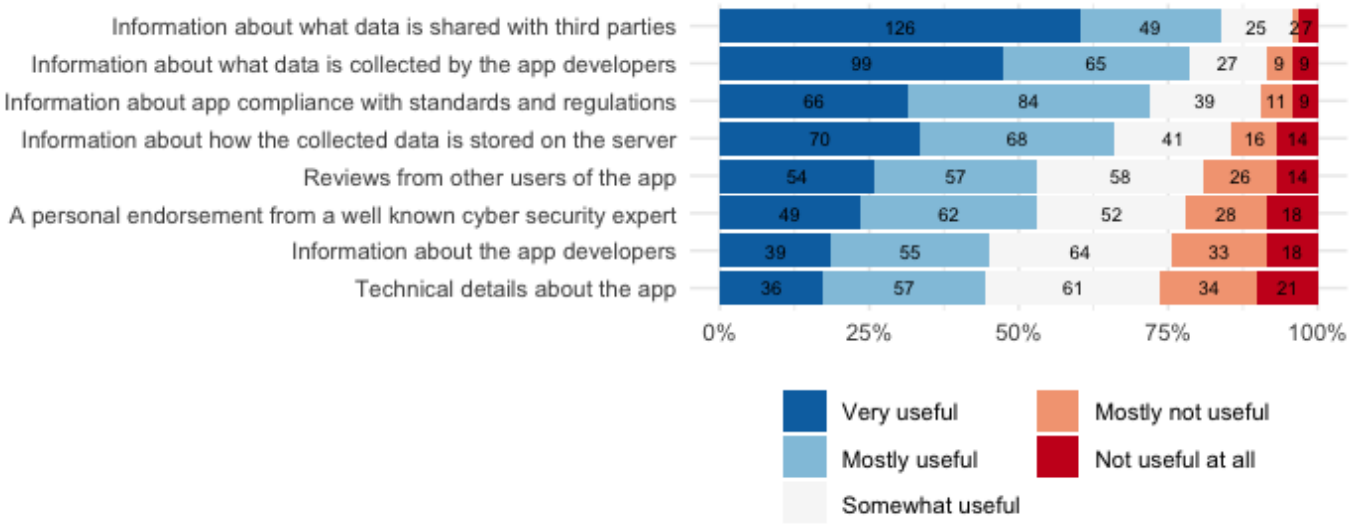

Fig. 2. Perceived usefulness of various types of information

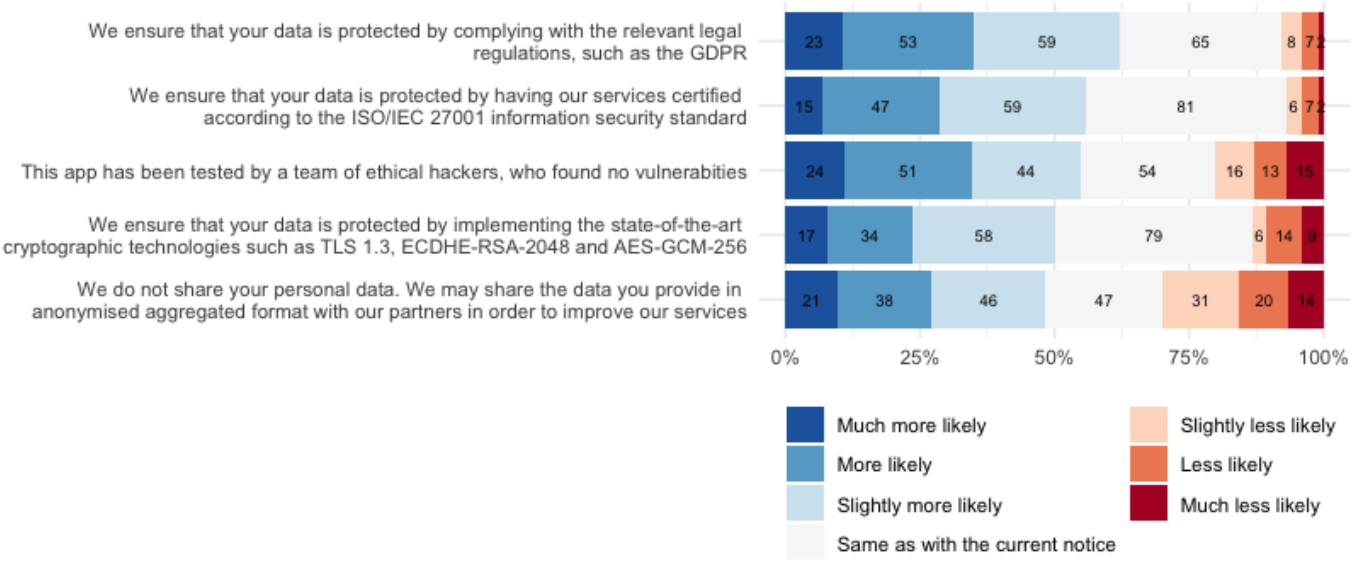

Fig. 3. Perceived likelihood of various types of assurances to lead to data disclosure

B. Study Procedure

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.

Fig. 4. Q-Sorting Process

Forty participants were recruited on the Prolific platform. This is consistent with recommended participant group sizes in Q-methodology [30]. 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 minutes of labour, exceeding the UK minimum wage. Participants did not provide any personal data, ensuring that participation was anonymous.

C. 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 [30]) (Figure 5). Factors 3 and 5 were eliminated because they had only 1 participant each.

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 can't 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 are not reassured by the website testing their website themselves: "*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.*"

Yet 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.*"

V. Discussion & Reflection

There are those who believe that people are resigned to privacy violations [31]. Our study suggests that this is

inaccurate. A number of reassurance statements appear on the far right (strong agree) on many factors. In particular: the statement saying that security experts have validated the security of the website seems to be particularly compelling.

None of the factors suggest that people avoid reading provided information because they do not understand how security is assured. Amongst participants, there was a hunger for reassurance and they seemed to want as much information as possible so that they could make an informed decision.

Solove [14] argues that "*Managing one's privacy is a vast, complex, and never-ending project that does not scale; it becomes virtually impossible to do comprehensively*" (p.3). Yet, users have not given up. Our findings confirm those of [32], who argue that "*consumers fundamentally care about online privacy*" (p. 736).

Research into the existence of the privacy paradox to resolve the current disagreement is required given its influence on privacy research. Choice architecture features of type 2, as shown in Figure 1, appear to exert the most influence. Hence, further studies into the best ways of formulating and presenting these would help online web services to know how best to reassure their users.

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' [33]. 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 [34]. 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*" [35], confirming the conclusions of [36]–[39]. Van der Velden [40] 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 amount of digital services people interact with on a daily basis. Our findings nonetheless show that users are interested in getting back control over their data. The fact that they often make decisions that negatively affect their privacy, however, points to the inadequacy of existing 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 [7]. A structural approach is required to address these deficiencies [41].

VI. Conclusion

The privacy paradox suggests that people only say that they care about their privacy, but then proceed to give their information away without seeming that worried about it. The first study's responses that led us to question this apparent indifference. Then, when we fed the outcome of their free-text responses into our Q-Methodology, we discovered that our participants *did* care about their privacy, and wanted reassurance that the organisation they were giving their information to was trustworthy. They wanted to be assured that the necessary measures had been put in place to secure their information.

The *research* implications of this are that the ubiquity and certainty of the privacy paradox should be questioned. It might well apply in some contexts but its influence is likely to be more nuanced and uncertain in other contexts. Certainly, more research needs to be undertaken into the applicability of the privacy paradox in a variety of contexts.

In *practical* terms, 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. They **do** care.

References

[1] Equality and Human Rights Commission, "Article 8: Respect for your private and family life," 2021, retrieved 19 June from: https://www.equalityhumanrights.com/en/human-rights-act/article-8-respect-your-private-and-family-life.

[2] O. Diggelmann and M. N. Cleis, "How the right to privacy became a human right," *Human Rights Law Review*, vol. 14, no. 3, pp. 441–458, 2014.

[3] A. F. Westin, "Social and political dimensions of privacy," *Journal of Social Issues*, vol. 59, no. 2, pp. 431–453, 2003.

[4] F. Kehr, T. Kowatsch, D. Wentzel, and E. Fleisch, "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, 2015.

[5] E. Aïmeur, O. Lawani, and K. Dalkir, "When changing the look of privacy policies affects user trust: An experimental study," *Computers in Human Behavior*, vol. 58, pp. 368–379, 2016.

[6] A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. di Vimercati, *What can behavioral economics teach us about privacy?* Auerbach Publications, 2007.

[7] D. J. Solove, "Privacy self-management and the consent dilemma," *Harvard Law Review*, vol. 126, pp. 1880–1903, 2013.

[8] K. Caine, S. Kohn, C. Lawrence, R. Hanania, E. M. Meslin, and W. M. Tierney, "Designing a patient-centered user interface for access decisions about EHR data: implications from patient interviews," *Journal of General Internal Medicine*, vol. 30, no. 1, pp. 7–16, 2015.

[9] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security*, vol. 64, pp. 122–134, 2017.

[10] T. Dienlin and S. Trepte, "Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors," *European Journal of Social Psychology*, vol. 45, no. 3, pp. 285–297, 2015.

[11] S. Barth, M. D. de Jong, M. Junger, P. H. Hartel, and J. C. Roppelt, "Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources," *Telematics and Informatics*, vol. 41, pp. 55–69, 2019.

[12] H. Li, X. R. Luo, J. Zhang, and H. Xu, "Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors," *Information & Management*, vol. 54, no. 8, pp. 1012–1022, 2017.

[13] A. Gruzd and Á. Hernández-García, "Privacy concerns and self-disclosure in private and public uses of social media," *Cyberpsychology, Behavior, and Social Networking*, vol. 21, no. 7, pp. 418–428, 2018.

[14] D. J. Solove, "The myth of the privacy paradox," *Geo. Wash. L. Rev.*, vol. 89, pp. 1–46, 2020.

[15] W. Hong, F. K. Chan, and J. Y. Thong, "Drivers and inhibitors of internet privacy concern: a multidimensional development theory perspective," *Journal of Business Ethics*, pp. 1–26, 2019.

[16] M. Jozani, E. Ayaburi, M. Ko, and K.-K. R. Choo, "Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective," *Computers in Human Behavior*, vol. 107, p. 106260, 2020.

[17] C. R. Sunstein and R. H. Thaler, *Nudge: Improving decisions about health, wealth, and happiness*. Penguin Books, 2014.

[18] G. Mazurek and K. Małagocka, "What if you ask and they say yes? Consumers' willingness to disclose personal data is stronger than you think," *Business Horizons*, vol. 62, no. 6, pp. 751–759, 2019.

[19] A. Beldad, T. van der Geest, M. de Jong, and M. Steehouder, "Shall i tell you where i live and who i am? factors influencing the behavioral intention to disclose personal data for online government transactions," *International Journal of Human-Computer Interaction*, vol. 28, no. 3, pp. 163–177, 2012.

[20] M. S. Kim and S. Kim, "Factors influencing willingness to provide personal information for personalized recommendations," *Computers in Human Behavior*, vol. 88, pp. 143–152, 2018.

[21] E. Xie, H.-H. Teo, and W. Wan, "Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior," *Marketing Letters*, vol. 17, no. 1, pp. 61–74, 2006.

[22] S. C. Robinson, "Factors predicting attitude toward disclosing personal data online," *Journal of Organizational Computing and Electronic Commerce*, vol. 28, no. 3, pp. 214–233, 2018.

[23] C.-H. Yeh, Y.-S. Wang, S.-J. Lin, T. H. Tseng, H.-H. Lin, Y.-W. Shih, and Y.-H. Lai, "What drives internet users' willingness to provide personal information?" *Online Information Review*, vol. 42, no. 6, pp. 923–939, 2018.

[24] J. M. Samens, "How individuals disclose health information: a study examining the choices made when sharing health information," Ph.D. dissertation, Communication, University of Wisconson-Milwaukee, 2017.

[25] M. Becker, C. Matt, and T. Hess, "It's Not Just About the Product: How Persuasive Communication Affects the Disclosure of Personal Health Information," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, vol. 51, no. 1, pp. 37–50, 2020.

[26] L. Coles-Kemp and E. Kani-Zabihi, "On-line privacy and consent: a dialogue, not a monologue," in *Proceedings of the 2010 New Security Paradigms Workshop*, 2010, pp. 95–106.

[27] W. Stephenson, "Correlating Persons Instead of Tests," *Journal of Personality*, vol. 4, no. 1, pp. 17–24, 1935.

[28] S. C. Weller, "Cultural consensus theory: Applications and frequently asked questions," *Field Methods*, vol. 19, no. 4, pp. 339–368, 2007.

[29] S. R. Brown, "A Primer on Q Methodology," *Operant Subjectivity*, vol. 16, no. 3/4, pp. 91–138, Apr. 1993.

[30] S. Watts and P. Stenner, "Doing Q methodology: theory, method and interpretation," *Qualitative Research in Psychology*, vol. 2, no. 1, pp. 67–91, 2005.

[31] N. A. Draper, "From privacy pragmatist to privacy resigned: Challenging narratives of rational choice in digital privacy debates," *Policy & Internet*, vol. 9, no. 2, pp. 232–251, 2017.

[32] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age," *Journal of Consumer Psychology*, vol. 30, no. 4, pp. 736–758, 2020.

[33] A. E. Waldman, "Cognitive biases, dark patterns, and the 'privacy paradox'," *Current Opinion in Psychology*, vol. 31, pp. 105–109, 2020.

[34] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 1326–1343.

[35] H. Malcolm, "Millennials don't worry about online privacy," 2021, https://eu.usatoday.com/story/money/business/2013/04/21/millennials-personal-info-online/2087989/.

[36] C. J. Hoofnagle, J. King, S. Li, and J. Turow, "How different are young adults from older adults when it comes to information privacy attitudes and policies?" *Available at SSRN 1589864*, 2010.

[37] N. M. Richards, *Four privacy myths*. Austin Sarat: Revised form, A World Without Privacy. Cambridge Press, 2015, forthcoming, Available at SSRN: https://ssrn.com/abstract=2427808.

[38] G. Blank, G. Bolsover, and E. Dubois, "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, 2014.

[39] H. Stanley, "Do young people care about privacy?" 2013, https://www.aclu.org/blog/privacy-technology/consumer-privacy/do-young-people-care-about-privacy.

[40] M. Van Der Velden and K. El Emam, ""Not all my friends need to know": a qualitative study of teenage patients, privacy, and social media," *Journal of the American Medical Informatics Association*, vol. 20, no. 1, pp. 16–24, 2013.

[41] J. S. Seberger, M. Llavore, N. N. Wyant, I. Shklovski, and S. Patil, "Empowering resignation: There's an app for that," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–18.

APPENDIX

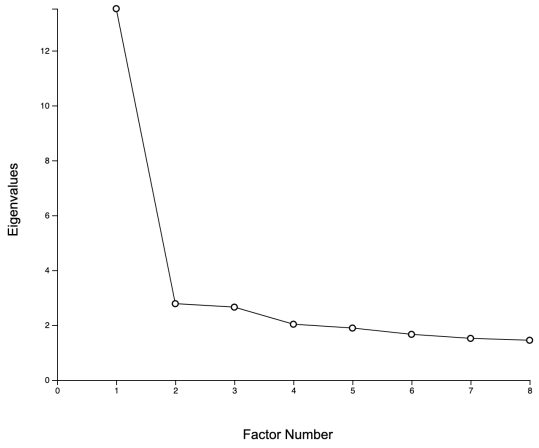

Fig. 5. Scree Plot

TABLE I

P-VALUES FOR POST-HOC TESTS FOR PERCEIVED USEFULNESS OF DIFFERENT INFORMATION TYPES (* SIGNIFIES STATISTICAL SIGNIFICANCE)

	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

TABLE II

P-VALUES FOR POST-HOC TESTS FOR PERCEIVED USEFULNESS OF DIFFERENT INFORMATION TYPES (* SIGNIFIES STATISTICAL SIGNIFICANCE)

	expert endorsement	compliance	storage of collected data	app developers	collected data	data shared with third parties	reviews from other users
comp-liance	*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

TABLE III

FINAL Q-STATEMENTS (STATEMENTS IN QUOTES) (SUBSCRIPTS REFER TO CLASSIFICATION IN TERMS OF FIGURE 1: 1=INDIVIDUAL RATIONALIZATIONS, (2) REASSURANCE STATEMENTS, (3) OBSERVATIONS BASED ON WEBSITE FEATURES)

1. "Your information is stored in a GDPR compliant way[2]"	20. Assurances only serve to worry me[1]
2. "Privacy International has accredited our website[2]"	21. My friends recommended this website to me[1]
3. "This website is WCAG compliant[2]"	22. If I see any assurance, I feel more protected[1]
4. "We will not sell or share your information with anyone[2]"	23. It depends on the kind of information that I am asked to share[1]
5. "Ethical hackers have tested this website and certified its security[2]"	24. "Vulnerabilities have been identified and eliminated"[2]
6. "We give you fine-grained controls over which of your data to share[2]"	25. I don't trust any assurances about encryption[1]
7. "For better security, you can activate two-factor authentication[2]"	26. I would never share my personal information regardless of assurances[1]
8. "Our reputation depends on us not violating your trust[2]"	27. Statements from well known security experts praising the website for good practice[1]
9. "Your information is encrypted using the Advanced Encryption Standard (AES)[2]"	28. The number of website customers who have ranked the website positively[1]
10. "We are ISO 27001 compliant[2]"	29. The more information that is provided, the more I likely would I would be trust them[1]
11. "We have industry standard measures in place to secure your information[2]"	30. If they ask for my consent, I would be more likely to trust them[1]
12. The website looks professional[3]	31. I don't want too much security information[1]
13. "We have never experienced an information breach"[2]	32. Life is too short to read all this information[1]
14. "We have an in-house security team monitoring our website 24/7[2]"	33. I have nothing to hide[1]
15. "We have repelled over 1000 cyber attacks in the last year[2]"	34. I don't trust anonymisation[1]
16. It doesn't matter what I see. I will use it[1]	35. "We anonymise all your information[2]"
17. I just have to trust any website because I don't understand security[1]	36. "We do not collect any non-essential information, only what we need to fulfill your order[2]"
18.The website's language is simple and easy to understand[3]	37. "Your information will be deleted as soon as the legally required retention period is over[2]"
19. The assurances have clearly been written by a lawyer[3]	38. The website provides a link to extensive information about security and privacy[3]