Google

Combining Personal Data under the DMA

1. Article 5(a) of the draft Digital Markets Act (**DMA**) stipulates that core platform services must "*refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services*" subject to users having "*been presented with the specific choice and provided consent*" to such combinations.

2. Recital 36 explains that Article 5(a) is designed to address "*potential advantages in terms of accumulation of data*" that core platform services might have and that could raise "*barriers to entry*" and "*unfairly undermine the contestability of core platform services.*" Article 5(a) therefore requires that gatekeepers should *"enable their end users to freely choose to opt-in to such business practices by offering a less personalised alternative."*

3. As a company, we have been engaging with privacy regulators and advocates—as well as with competition authorities, academics, and other stakeholders—on the way we collect and use personal data. We have also been thinking about these issues internally as part of our policy and design decisions, both in our user-facing services and in how we build our systems. Google therefore welcomes the DMA as an opportunity to bring fact-driven clarity to these issues.

4. We agree that combining personal user data across services must be done responsibly and that users should be given effective opportunities of choice and control. At the same time, user consent moments must be implemented in a proportionate manner to avoid overloading users and undermining beneficial product developments.

5. We hope the DMA will provide a coherent, pan-European framework that balances and reconciles these different considerations based on thoughtful, evidence-based enforcement. We're looking forward to discussing our current approach with the Commission and working collaboratively together to identify areas where we can do more.

6. This paper explains our thinking on the matters covered in Article 5(a). We discuss five key principles that ought, in our submission, govern the application of this provision:

Principle 1: Subject to appropriate user control, the legitimate combination of personal data can bring tremendous user benefits.

Principle 2: Consent moments should match users' expectations and provide them with real control, not overburden or confuse them.

Principle 3: Consent should not inhibit essential product safety functions.

Principle 4: Compliance with Article 5(a) ought to build on existing compliance frameworks already developed for complying with the GDPR.

Principle 5: Article 5(a) should be applied coherently throughout the EEA.

7. These principles would contribute to a proportionate enforcement framework for Article 5(a). They limit the risk that Article 5(a) inadvertently harms consumers by denying them access to integrations they expressly request or expect. And they prevent overwhelming users with an unmanageable avalanche of repeated pop-up consents that would frustrate them and would lead to users ignoring consent moments—so-called consent "blindness". At the same time, these principles do not impair the DMA's objective of preventing personal data aggregation that allegedly raises barriers to entry. This short paper provides Google's perspective on these principles and explains why we believe they are important to the success of the enforcement of Article 5(a).

8. We believe that the principles that we discuss in this paper follow from the DMA's overall rationale and the fundamental principle of proportionality. For clarity, we provide, at the end of this paper, suggested amendments to Art. 5(a) that would make these principles explicit. We look forward to discussing together the points covered in this paper and the application of the DMA more broadly.

Principle 1: Legitimate personal data combination subject to appropriate user control can be beneficial for users.

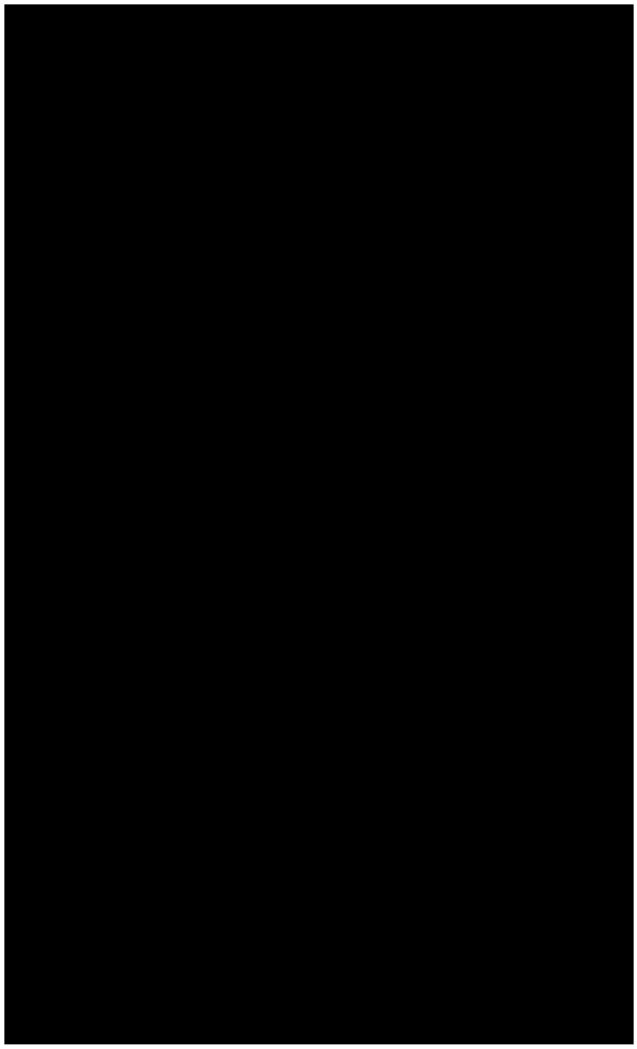
9. Some commentators argue that Article 5(a) ought to preclude gatekeepers from combining *any* personal data, even when users want and ask them to do so. This position wrongly assumes that all combinations of personal data are inherently harmful. This is an incorrect premise on which to rely when thinking about the drafting or enforcement of Article 5(a).

10. [redacted]

[redacted]

- [redacted]

- [redacted]



- [redacted]

[redacted]

11. We do not think it would be right for the DMA to prevent users consenting to combine their data to receive enhanced services. Evidence shows that users value thoughtful personalization and product integrations.[1]

12. Users should have the choice to access their personal data across services where doing so can, in their own view, benefit them. We hope that the DMA will not take the

[1] Third-party research shows that users welcome thoughtful personalization. For instance, a 2017 study by Epsilon concluded that 90% of respondents find personalization appealing (see Epsilon, Research summary, 9 January 2018); a report by consulting firm Accenture found that 91% of consumers say they are more likely to shop with brands that provide offers and recommendations that are relevant to them, while 74% of consumers say "living profiles" with more detailed personal preferences would be useful if they were used to curate personalised experiences, products and offers (see Accenture, Pulse Check 2018 Report, 2018); an Adobe consumer survey found that 67% of consumers believe that it is important for brands to automatically adjust content based on their current context to provide a real-time personalised experience (see CMO by Adobe, Consumer demand for personalized content reaches all-time high, 6 January 2018).

unnecessary and harmful additional step of limiting—rather than preserving—users' control over their personal data.

13. We also appreciate that Article 5(a) is not just about privacy outcomes, but is also designed to alter the competitive process within online markets. But such efforts should also be proportionate and reflect users' best interests. An outright ban on personal data combinations, however, is not a proportionate means to improve the competitive process.

- **A ban would harm users.** Improving the competitive process should be to the ultimate benefit of consumers. But an outright ban on combining personal data would harm not benefit consumers. The ban would reduce users' options and control. It would remove users' ability to choose to obtain enhanced features they like while giving them nothing in return. And it would force us to remove beneficial features and services that users like and value, including security services, efficient and effective privacy controls, and value-added cross-service experiences.

- **A ban would distort competition.** A ban on combining personal data would prevent gatekeepers from offering a service that rivals could continue to offer. This would not create a level-playing field. It would create an artificial quality degradation of gatekeeper services. And it would limit output and innovation. Such a ban would therefore exceed the DMA's stated objective and result in a disproportionate restriction. Cross-service data access *subject to user consent* achieves the goals specified in Recital 36 because the purpose of Article 5(a) is to address "*potential advantages*", not create disadvantages.[2]

14. In our view, the key for achieving the DMA's objective in a manner that does not harm users or distort competition is to ensure that users enjoy real, easily accessible choice. Google therefore considers that limitations in Article 5(a) on cross-service data sharing should always be subject to such choice.[3] Thoughtfully enforced in line with the other principles below, we believe this approach is a source of potential clarity and coherence on an important topic.

Principle 2: Consent moments should match users' expectations and provide them with real control, not overburden or confuse them.

15. We already provide users with a range of granular privacy settings and controls through which users can manage Google's processing of their personal data. These controls include options that provide users with the choice to enable or disable

---

2 In fact, the current draft of the DMA already goes further than creating a level-playing field because gatekeepers can only use the consent basis under the GDPR for sharing personal data across services, but not the other legal bases (such as processing personal data by reference to legitimate expectations or to make good on contractual requirements).

3 Recent proposals by ITR Committee in the European Parliament on Article 5(a) are sensitive to this notion since they appear to seek to enable pro-competitive combinations and to give users control by enabling them to consent to specific combinations they find useful.

particular personalization features or the recording of particular data types while retaining the ability to use the service in question.[4]

16. We are ready to expand on these options to give users even more control over the cross-service use of their data. At the same time, consent moments should match users' expectations and provide them with real control, not overburden or confuse them.

17. This is an important issue. Evidence from our own experience and from studies in peer-reviewed scientific journals shows that increasing the number of choices available to users does not always result in real added choice. An excessive range or recurrence of choice moments leads to friction in expressing preferences and to "consent blindness". As a result, more choice points may, in fact, lead users to interact less with their privacy controls.

18. For instance, several studies looking at the real-world impact of cookie-consents mandated by the GDPR concluded that more consents did not equate to more engagement.[5] Rather, they found that most users were annoyed by the cookie disclaimer; the consent moment is a nuisance to users' enjoyment of the web; and most users simply accept cookie disclaimers blindly to get rid of them.[6]

19. Other studies have corroborated these findings. Several studies on "choice architecture" conclude that participants assigned large numbers of choices are less satisfied with their choices made, experience more regret, and are overwhelmed by decision process than participants shown a smaller range of more meaningful choices. These studies suggest that increasing the number of options or information density has a cost to users and does not lead to more engagement with the offers; quite the opposite, it leads to less engagement.[7]

20. These studies correspond to our own findings. This is why we seek to design our privacy controls in line with likely user expectations and by incorporating feedback from user testing [redacted]

---

4 Google provides additional details on these controls in Annex 1.

5 Google provides in Annex 2 a digest of recent academic literature on this topic. Section 1 of Annex 2 lists literature regarding cookie consents.

6 This is discussed in the 2017 study "*This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer*": the follow up 2018 study on a longer time period; and a 2019 study on the same issue "*(Un)informed Consent: Studying GDPR Consent Notices in the Field,*" see Annex 2 for further details.

7 Google provides detail on a range of choice architecture studies in Section 2 of Annex 2.

[redacted]

21. This approach helps us try to balance the options we provide with the need to make the exercise of choice meaningful for users and avoid overwhelming users with complexity.

[redacted]

- For data with higher sensitivity, we provide stricter protections and more extensive controls.

22. The evidence is clear: while users want control over their personal data, they do not want to be bombarded with an array of buttons and consent boxes that require their time and attention before they can access services and features they value. The DMA will affect the balance of what consents are shown to users -- we believe it should do so in a manner that does not reduce the effectiveness of users' choice by overwhelming them with prompts and options or by ignoring their clear intentions.

Principle 3. A requirement to obtain consent should not inhibit essential security functions.

23. As we described above, an important use-case for cross-product personal data sharing today is ensuring users' and our systems' security and safety.

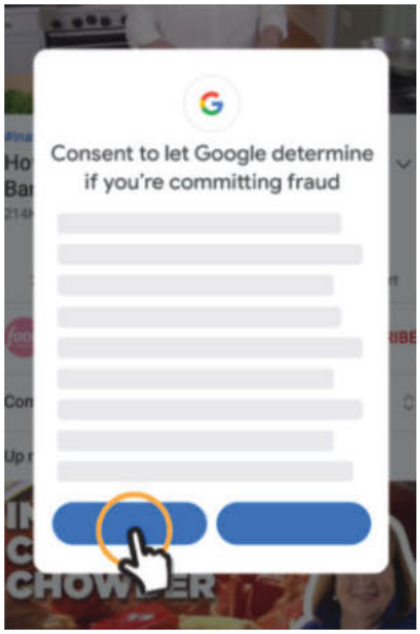
24. Our systems and our users are under constant attack from bad actors. Examples of these sort of attacks include attempts to invade user privacy (e.g. via malware or phishing), fraud (e.g. via click-fraud on ads), or attacking Google's ability to offer its services to users (e.g. via a distributed denial of service attack).

25.

[8]

- [redacted]
- [redacted]
- [redacted]

[redacted] It would be unreasonable to expect Google and other companies to seek fraudsters' consent to detect such fraudulent accounts. Were this the case, it is more likely they would actively use that consent as a loophole to evade detection The DMA should expressly exclude personal data usage for such purposes from its scope. Or, failing that, the application of the DMA should not require us to show consent moments like the one below.



Principle 4. Compliance with Article 5(a) ought to build on existing data protection frameworks already developed for compliance with the GDPR and other internal and external requirements.

27. We explained above that we provide users with control and choice over the use of their data. Internally our systems are built to ensure we respect the choices that users make. On occasion, we've heard third parties suggest that personal data within

Google is subject to a "free-for-all."[9] These claims do not reflect reality, they are plain wrong. As part of compliance with the GDPR and our broader commitment to protecting user data, we have developed a systematised data-protection framework for personal data.

28. The basis of this framework is [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

9 https://brave.com/google-internal-data-free-for-all/.

[redacted]

32. **Enforcement.** [redacted]

33. This is not to say that our controls cannot be improved upon -- we have large engineering teams dedicated to their operation and enhancement. Nor is it to say that these systems will not need to be adapted to ensure compliance with Article

5(a). [redacted]

34. At the same time, however, the DMA should not require a de-facto reinvention of the compliance mechanisms we use today. We hope that DMA enforcement can take place by building on the powerful tools we already have and we stand ready to explain these tools in more detail to the Commission's services.[10]

Principle 5: The application of Article 5(a) should be coherent throughout the EEA.

35. We are concerned about calls for the fragmentation of the enforcement of the DMA. As the points made necessarily imply, we expect compliance with the DMA to involve in-depth and frequent engagement with the regulator responsible for the DMA's implementation. As a company, we are committed to engaging with that regulator in technical detail and in a transparent manner.

36. [redacted] In all probability, we will have to implement these changes on a worldwide basis. It is not practicable to maintain different designs, processes, and infrastructure for such fundamental issues as data flows and controls.

37. It is therefore critical to have a unified and consistent application of the DMA, especially for rules regulating data flows. Frequent, unjustified change to the interpretation of the DMA or -- worse still -- fragmentation of enforcement across member states would make compliance impossible. Advocates of this type of enforcement fail to understand the scale of the implications of this law for our company, employees, systems, and users.

38. We cannot manage data one way in France and another way in Germany. We cannot develop different technical infrastructure to reflect different consent standards across different jurisdictions or use data to fight fraud one day but cease that usage the next.

39. The DMA is too far reaching to be fragmented. And fragmentation would be directly opposed to the stated objective of achieving harmonisation across Europe.

Conclusion

[10] There is also a relationship between Principles 4 and 5: the more complex the consents the DMA requires gatekeepers to present to users, the more complex the implementation of the users' choices in internal systems. Each consent permutation provided to the user in the frontend of a Google service triggers the need to replicate that permutation in the logic in the back-end of our systems. The more permutations, the more complexity in the back-end logic. Enforcing excessively granular consent options in our backend would become increasingly difficult and prone to error.

40. We understand the purpose of Article 5(a) and agree with the basic concepts it embodies. Applying the DMA consistently with the five principles that we have outlined in this paper can both meet the DMA's objectives and avoid harming legitimate interest:

    1. Subject to appropriate user consent, the combination of personal data can bring tremendous consumer benefits

    2. Consent moments should match users' expectations and provide them with real control, not overburden or confuse them

    3. Consent should not inhibit essential security functions

    4. Compliance with Article 5(a) ought to build on existing compliance frameworks already developed for complying with the GDPR

    5. Article 5(a) should be applied coherently throughout the EEA

41. These principles, in our submission, follow directly from the DMA's rationale and the fundamental principle of proportionality. Nonetheless, to avoid misunderstandings, especially when confronted with the risk of fragmented interpretation of the text, it would be helpful to enshrine the five principles through the following textual amendments:

    Gatekeepers shall "*refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with* ~~*the specific*~~ ***a*** *choice* ***that is practicable and in line with reasonable user expectations, and the user*** *provided consent in the sense of Regulation (EU) 2016/679.* ***This requirement does not apply to gatekeepers combining such data for the purposes of detecting/combating fraud, abuse, or other safety-related activity, where compelled by law, or where the primary purpose of the user providing their data to the gatekeeper is for their data to be shared across services.***

42. At a minimum, we hope that the current text of the Article can be applied in a manner that is sensitive to the principles we have outlined today.

Annex 1

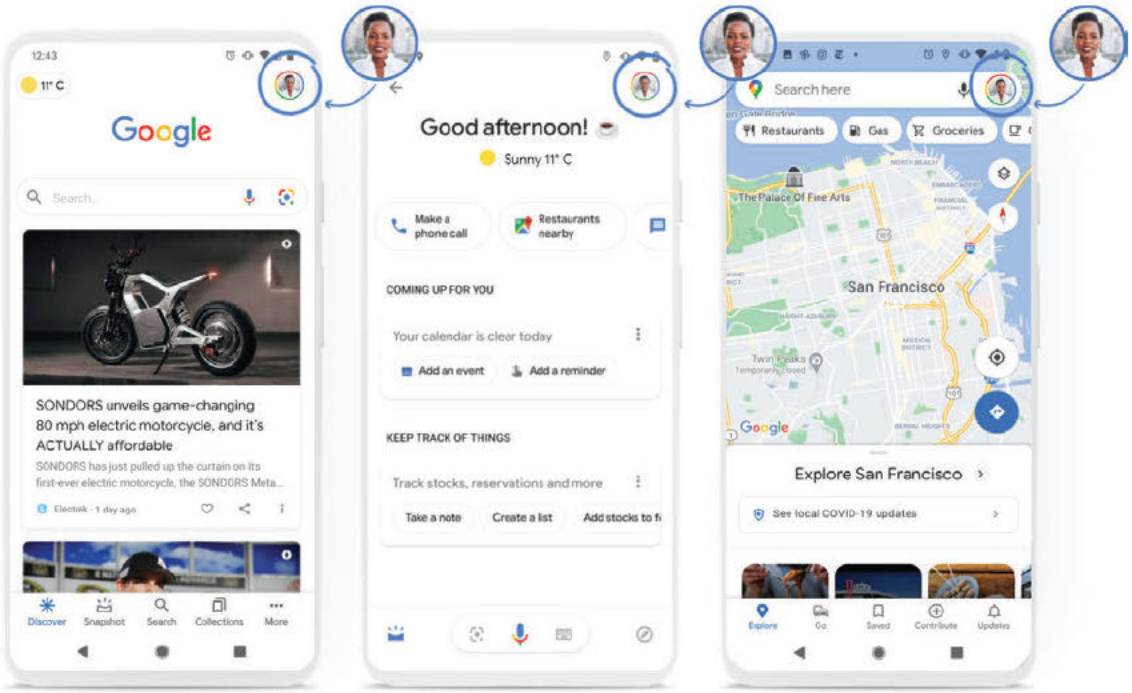
Overview of the controls Google makes available to users

1. Users have a number of ways to control and manage Google's processing of their data, including processing of data across services. These options include: (i) privacy settings and controls; (ii) switching between logged-in and non-logged in status; (iv) using multiple accounts; (iv) private browsing; (iv) and data deletion.

2. **Privacy settings and controls.** Google provides a range of granular privacy settings and controls through which users can manage Google's processing of their data. These controls include options that provide users with the choice of enabling or disabling particular personalization features or the recording of particular data types while retaining the ability to use the service in question.

3. To facilitate access to, and use of these tools, Google has centralised them in an easily accessible privacy hub. Centralization of these controls enables users to set preferences across Google services from a single space. [redacted]

Where do you go in product to find out what Google knows about you?



Search Assistant Maps

4. Google has designed the privacy controls it offers within the hub (and beyond it) in line with likely user expectations and incorporating feedback from user testing. It has also carefully balanced the options it provides with the need to make the exercise of choice meaningful for users and avoid overwhelming users with complexity. [redacted]

[redacted]

5. For example, [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

8. Through these settings, both signed-in and signed-out users have considerable control over the manner in which Google processes their data.

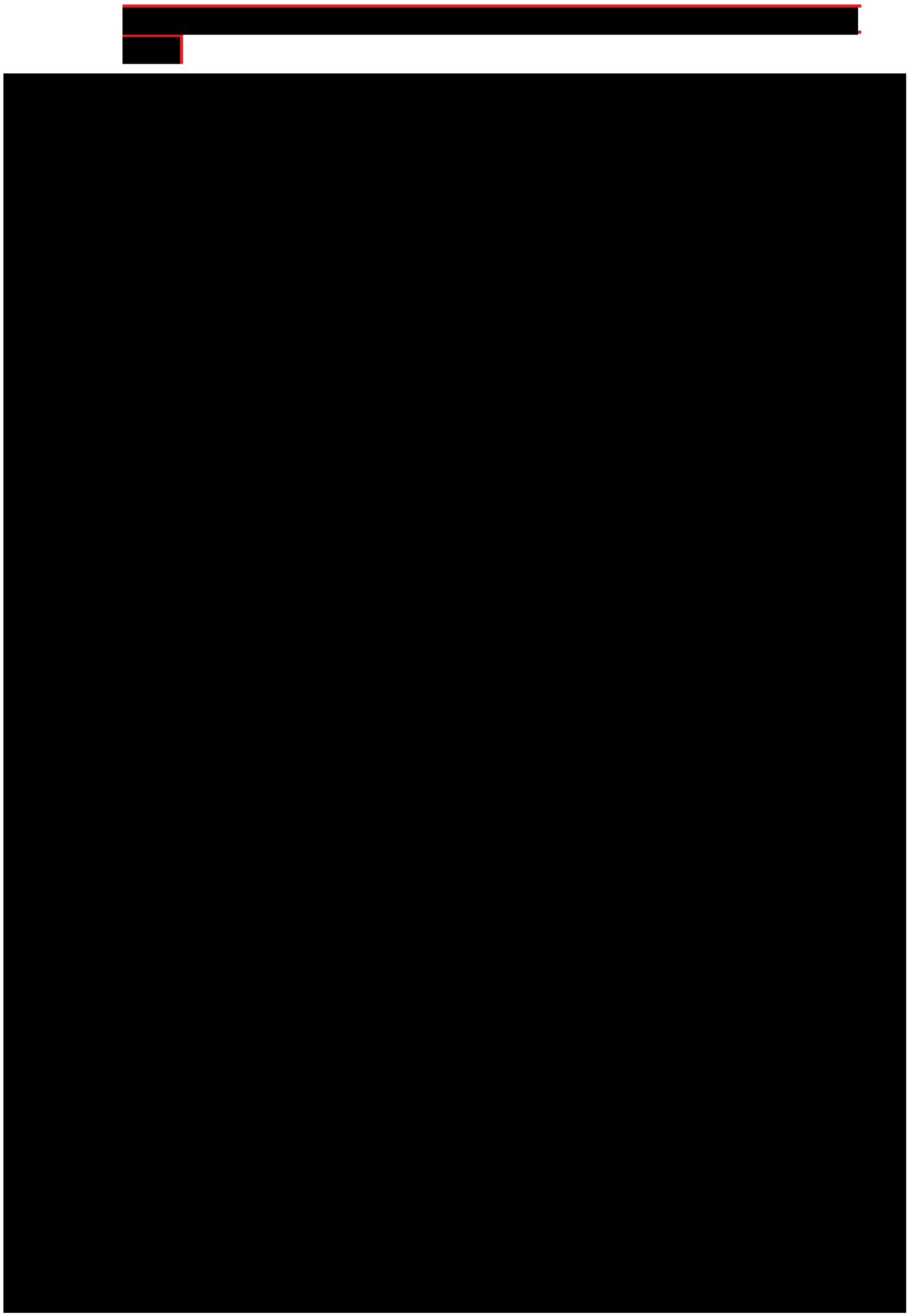
9. [redacted]

[redacted]

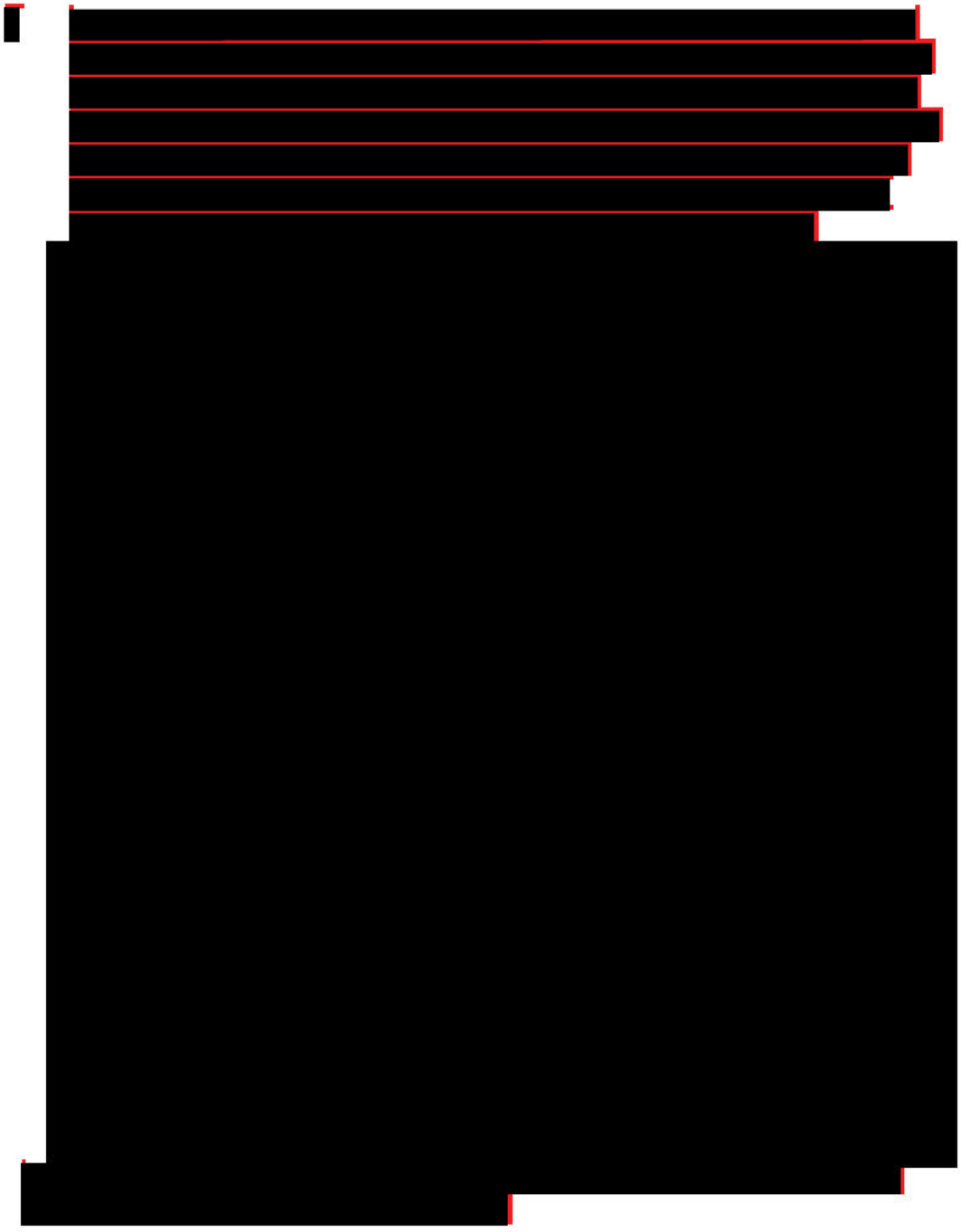
- [redacted]

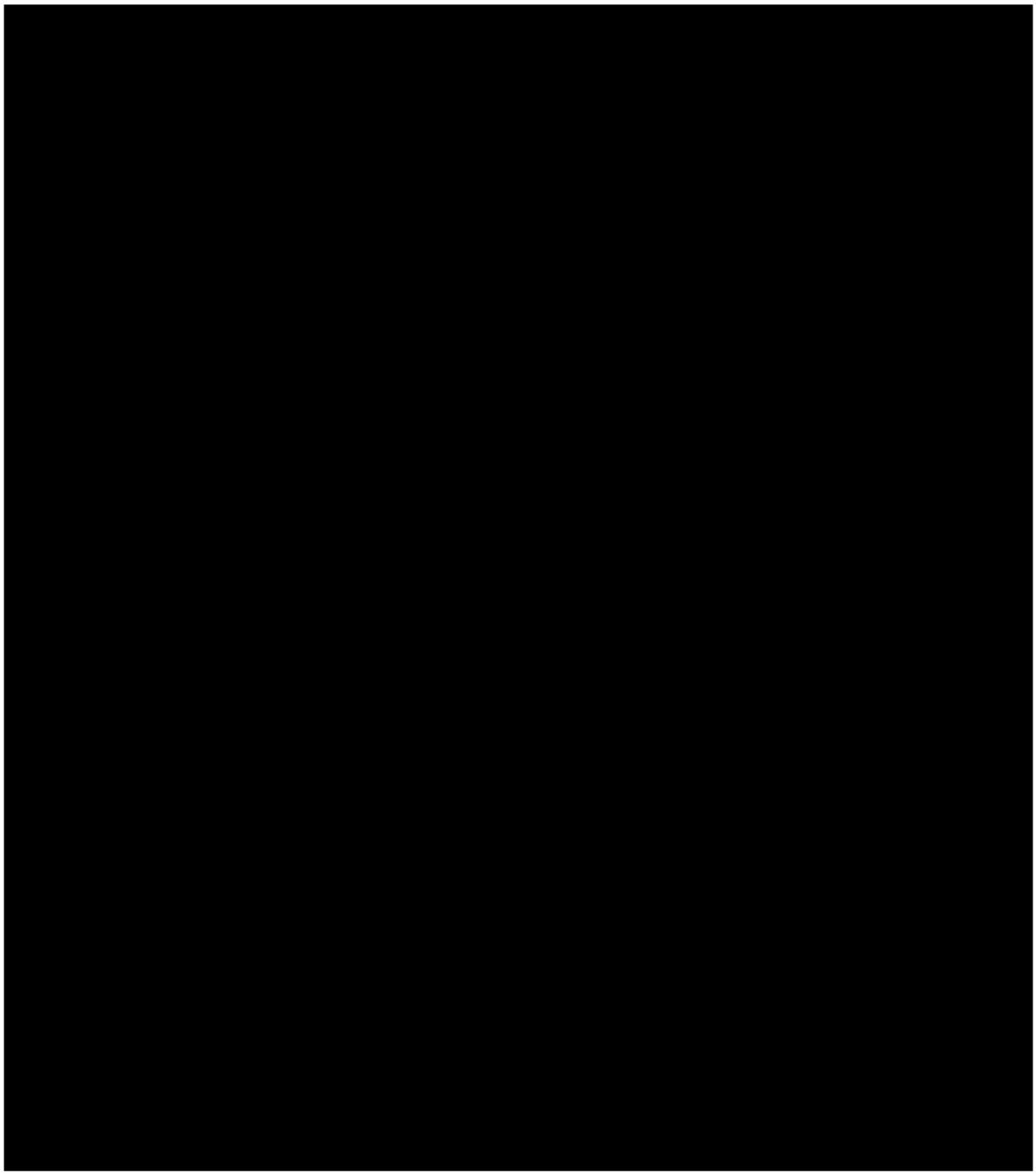
[redacted]

- [redacted]



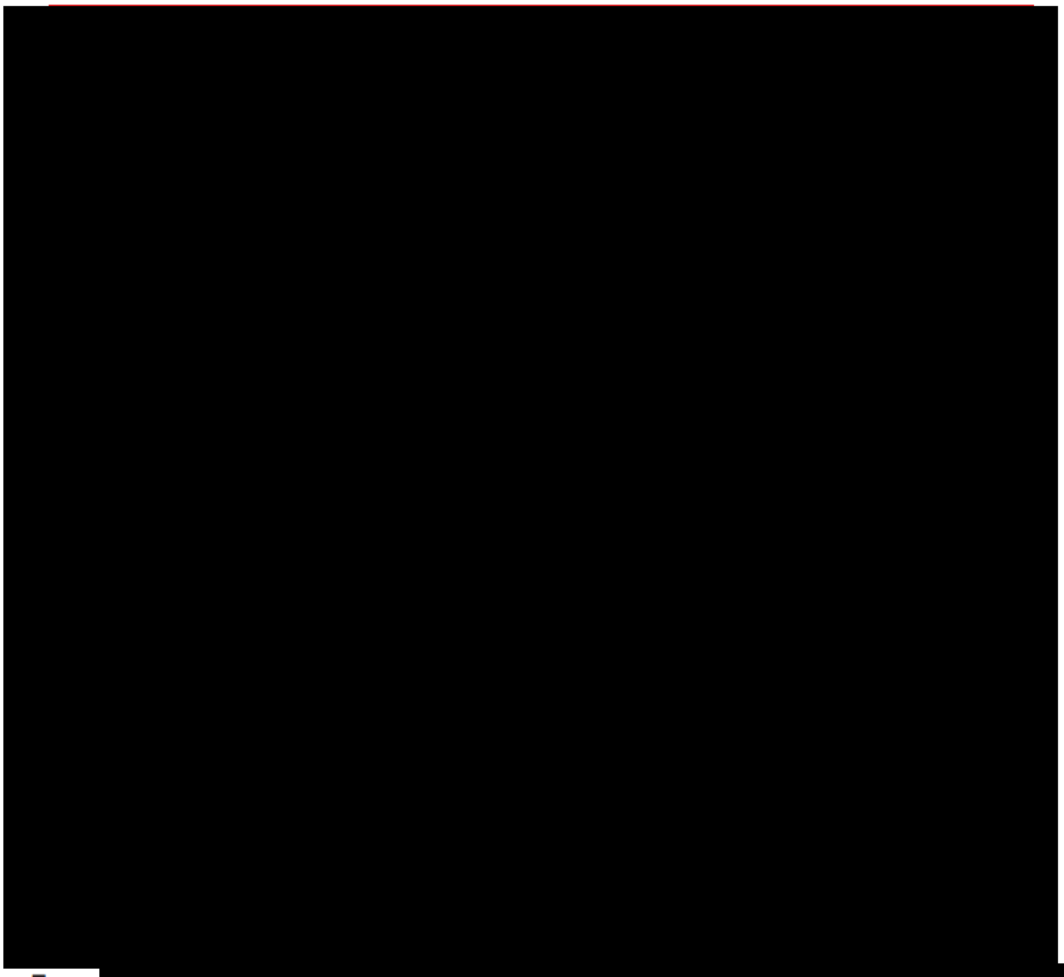
10. [redacted]





- [redacted]

- [redacted]



- [redacted]

[redacted]

11. [redacted]

- [redacted]
- [redacted]
- [redacted]

Annex 2

This Annex provides an overview of empirical studies by third-party academic researchers regarding the impact of different types of consent options on user engagement.

1. Empirical studies on the effect of EU cookie consents (ePrivacy Directive) on user task performance, satisfaction, fatigue, habituation.

1.1. Kulyk, O; Hilt, A.; Gerber, N., & Volkamer, M. (2018). "*This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer.* In: 3rd European Workshop on Usable Security (EuroUSEC), London, England. Retrieved from: https://www.ndss-symposium.org/wp-content/uploads/2018/06/eurousec2018_12_Kulyk_paper.pdf

This study, an online survey (N=150), investigated users' perceptions of cookies when seeing the cookie disclaimer, the users' reactions to such a disclaimer and different factors that influenced the users' decision to leave or continue using the website.

Answers from participants were grouped into these categories: disturbance, privacy, concern, habituation, misconceptions, lack of information.

Disturbance: A large number of the participants claimed to be annoyed by the cookie disclaimer, as they considered it a disturbance in their surfing: "As these messages appear constantly, I find them to be disruptive and annoying".

Privacy Concerns: Another common theme was the concern of the users regarding their privacy: "I feel myself observed".

Habituation: Due to prominence of cookie disclaimers, many participants claimed to be used to it and not to pay much attention to the disclaimer. As such, many reacted in a neutral way to the disclaimer. At the same time, a number of participants still claimed to have negative feelings towards cookie use. Still, as they felt that there was no way to avoid it, they admitted to being resigned in their attempts to act against it: "As this is the case with so many websites, I don't have much thoughts anymore regarding these cookies. [...] One feels somewhat helpless, but I seldom have this feeling and it is not so strong. When it comes to privacy protection in the internet (where cookies also belong), I've rather resigned myself".

The results showed that a large part of the participants considered the cookie disclaimer as a nuisance in their surfing rather than useful means for providing information about the cookie usage.

The study furthermore revealed that the text of the disclaimer did not play a significant role in users' decision, with more important factors being, instead, the reputation of the website and the type of service or content it provided

(and its importance to the user). At the same time, many participants claimed to have privacy concerns regarding cookies.

1.2. Kulyk, O; Hilt, A.; Gerber, N., & Volkamer, M. (2020). *Has the GDPR hype affected users' reaction to cookie disclaimers? Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa022

This study was conducted December 2018 as follow-up to the 2017 study to assess any impact on users' sensitivity to privacy protection of the extensive media coverage of data protection issues that accompanied the EU General Data Protection Regulation (GDPR) entry into force in May 2018.

The study concluded that the GDPR did not lead to users being more concerned about their privacy due to cookie disclaimers, nor did it lead to users rejecting the cookie collection more often.

Even more participants reported accepting cookie disclaimers in the follow-up study compared to the original, whereas fewer said they would leave the website if they were confronted with a cookie disclaimer.

Significantly more participants said that they felt disturbed by the disclaimer, while, at the same time, more participants were used to seeing the disclaimer and fewer were concerned about their privacy. In line with this, significantly less participants of the follow-up study stated that their decision to leave or stay on the website depended on how important the content of the website and how trustworthy the website was. Hence, it seems that even more users tended to accept cookie disclaimers blindly to get rid of them, which may be an unintended side-effect of the increasing use of cookie disclaimers on websites due to the introduction of the GDPR.

Results suggest that users did not change their attitude towards cookie use in favour of privacy protection, but got even more accustomed to the use of cookies, also by third parties.

The results of the study imply that superficial measures to inform users about data collection can disincentivize the users from taking measures to protect their privacy, as they feel more overwhelmed with the amount of decisions they have to make and feel more convinced about the futility of privacy protection.

1.3. Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* . Retrieved from https://dl.acm.org/doi/10.1145/3319535.3354212

Reasons for (Non-)Interaction with cookie consent notices:

- 61/100 participants clicked on the consent notice; out of these (multiple choice):
- 44 reported they had done so because they were annoyed by it.
- 16 thought the website would not work otherwise
- 13 stated they had clicked the notice out of habit.
- 11 participants interacted with the notice to protect their privacy,
- 6 for security reasons,
- 5 to see fewer ads.

Recurring themes in open-end responses include that the notices were "annoying [...], so I just ignore them out of frustration"

2. Increasing the number of options or information density (e.g. in a menu or search results page) has a cost to users in terms of task performance, cognitive load, product satisfaction, choice satisfaction, understanding of choices offered, quality of choices made, perceptions of usability, etc.

    2.1. Oulasvirta, A., Hukkinen, J.P., & Schwartz, B. (2009). When more is less: the paradox of choice in search engine use. In Proceedings of the 32nd international ACM SIGIR conference on Research and development in information retrieval (SIGIR '09). Association for Computing Machinery, New York, NY, USA, 516–523. DOI: https://doi.org/10.1145/1571941.1572030

    In numerous everyday domains, it has been demonstrated that increasing the number of options beyond a handful can lead to paralysis and poor choice and decrease satisfaction with the choice. Were this so-called paradox of choice to hold in search engine use, it would mean that increasing recall can actually work counter to user satisfaction if it implies choice from a more extensive set of result items.

    The existence of this effect was demonstrated in an experiment where users (N=24) were shown a search scenario and a query and were required to choose the best result item within 30 seconds. Having to choose from six results yielded both higher subjective satisfaction with the choice and greater confidence in its correctness than when there were 24 items on the results page.

    The finding was discussed in the wider context of "choice architecture"--that is, how result presentation affects choice and satisfaction.

    2.2. Korff, S., & Böhme, R. (2014). Too Much Choice: End-User Privacy Decisions in the Context of Choice Proliferation. *SOUPS*. Retrieved from https://www.usenix.org/system/files/soups14-paper-korff.pdf

This study provides initial empirical evidence of negative psychological effects triggered by the proliferation of choice in a privacy context. The authors used elements of decision field theory, consumer psychology and findings of Too Much Choice (TMC) research in order to devise a model that illustrated selected aspects of a disclosure decision.

Results showed that participants assigned to a large choice condition reported to be less satisfied with their choices made, experienced more regret, and were more overwhelmed by the decision process.

Despite some limitations, the results demonstrated that the number of privacy options presented to a user affects the (short-term) emotional reflection of the decision in the evaluation phase of a decision-making process.

2.3. Chiravirakul, P. & Payne, S.J. (2014). Choice overload in search engine use? In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14). Association for Computing Machinery, New York, NY, USA, 1285–1294. DOI: https://doi.org/10.1145/2556288.2557149

In this paper a series of three experiments was conducted to investigate the choice overload effect in search engine use. Participants were given search tasks and presented with either six or twenty-four returns to choose from. The results revealed that the choice behaviour was strongly influenced by the ranking of returns, and that choice satisfaction was affected by the number of options and the decision time.

The main results, from the third experiment, showed that large sets of options yielded a positive effect on participants' satisfaction when they made a decision without a time limit. When time was more strongly constrained, choices from small sets led to relatively higher satisfaction.

These studies show how user satisfaction with found information can be affected by processing strategies that are influenced by search engine design features.

2.4. Bollen, D. G. F. M., Knijnenburg, B. P., Willemsen, M. C., & Graus, M. P. (2010). Understanding choice overload in recommender systems. In *RecSys '10 : Proceedings of the fourth ACM Conference on Recommender systems, September 26-30,2010, Barcelona. Spain* (pp. 63-70). Association for Computing Machinery, Inc. https://doi.org/10.1145/1864708.1864724
(Note: Full text is not publicly accessible)

Even though people are attracted by large, high quality recommendation sets, psychological research on choice overload shows that choosing an

item from recommendation sets containing many attractive items can be a very difficult task. A web-based user experiment using a matrix factorization algorithm applied to the MovieLens dataset was used to investigate the effect of recommendation set size (5 or 20 items) and set quality (low or high) on perceived variety, recommendation set attractiveness, choice difficulty and satisfaction with the chosen item. The results show that larger sets containing only good items do not necessarily result in higher choice satisfaction compared to smaller sets, as the increased recommendation set attractiveness is counteracted by the increased difficulty of choosing from these sets. These findings were supported by behavioral measurements revealing intensified information search and increased acquisition times for these large attractive sets.

2.5. Tsun-Yin (Tracie) Tung, Leslie Davis Burns, and Harold F Koenig. 2019. Choice Overload and Online Approach Behavior. Int. J. E-Bus. Res. 15, 4 (Oct 2019), 56–72. DOI:https://doi.org/10.4018/IJEBR.2019100104
(Note: Full text is not publicly accessible)
This study examines how the number of choices offered on a website influences consumers' internal states (affective and cognitive responses) and their approach/avoidance behavior during online apparel shopping. Focus-group and questionnaire data collection methods with a 3 (number of choices) by 3 (presentation formats) factorial experimental design were employed. The theoretical frameworks, “choice overload” and “online store atmospherics and shopper response,” were applied. A total of 382 usable responses were collected. Although the interaction proposed in the study was not statistically significant, the findings of the study show that the effect of choice overload may not only influence the in-task generated responses but also have a deeper and long-lasting impact on the online consumer behavior. The respondents react to the large choice set on the basis of feelings and emotions (affective responses), and these responses ultimately lead to a subsequent attitude and approach behavior.

Annex 3

[redacted]

1. [redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

- [redacted]
- [redacted]

- [redacted]
- [redacted]