End-Users and Service Providers: Trust and Distributed Responsibility for Account Security

Yomna Abdelaziz
Carleton University
yomna.abdelaziz@carleton.ca

Daniela Napoli
Carleton University
daniela.napoli@carleton.ca

Sonia Chiasson
Carleton University
chiasson@scs.carleton.ca

***Abstract*—In a between-subjects study design, we compared responses from 170 online account users of two major service providers to explore issues relating to responsibility and trust for account security. Participants attributed clear roles between themselves and their service providers for preventing attacks, monitoring their accounts, and recovering their accounts. The emerging mental model of distributed responsibility does not match service providers stated terms of use. Users identified a variety of reasons for trusting different service providers, but reputation was viewed as especially important.**

I. Introduction

When considering online security measures, where does the service provider's responsibility end and the user's responsibility begin? Why do users trust online service providers? For users to safely enjoy an online service, personal information, usage content, and usage data must be protected. However, when users' expectations are violated, this could lead to a decline in their trust for the service provider.

In recent years, users of two major service providers (SPs), Facebook and Google, have faced disappointments regarding their privacy. In 2013, users filed a lawsuit against Google because Gmail scans their emails for advertising purposes [1]. Although Google was not violating the terms of service, it was the mismatch in expectations that lead to those users mistrusting their service provider. The 2018 Cambridge Analytica scandal [2] for Facebook similarly shook users' confidence in their service provider. Due to these developments, we choose to focus on Facebook and Google to understand how users perceive their relationship with these service providers. This target demographic is significant as Facebook has 2.23 Billion active users as of June 2018 [3], and Google, has seven products with over 1 Billion active users each as of May 2017 [4]. To place these numbers into perspective, there are an estimated 4.1B internet users worldwide in 2018 [5].

Realistically, both the service provider and the user play proactive and reactive roles in protecting users' online security and privacy. For context, proactive measures are steps taken to prevent attacks before they happen, *e.g.*, using two-factor authentication or using a password manager to generate strong passwords [6]. Online service providers take proactive security measures to keep user accounts safe by employing robust technology to prevent unauthorized access [6]. Reactive security measures are steps taken to recognize potential attacks or to recover and/or prevent further damage to accounts after an attack, *e.g.*, cancelling one's credit cards after detecting unauthorized account access, or monitoring accounts for failed access attempts. One way that online service providers take reactive security measures is by monitoring user accounts for suspicious activity [6]. Given the nature of security threats, proactive measures are unlikely to mitigate all risks (such as phishing [6]), and reactive measures should also be in place to respond to incidents.

For this paper, our main goal is to explore how users view their role and their SP's role in maintaining account security. To achieve this, we pose two research questions:

RQ1. Who do users perceive is responsible for preventing attacks, monitoring their accounts, and recovering their accounts?

RQ2. What *trust cues* make online service providers (SP) trustworthy to users?

The first question provides insight regarding which circumstances users assume a passive or active security management role. It also allows us to compare how user mental models align with the services they are provided. The second question helps us to understand why users trust service providers when externalizing the responsibility of account security.

To explore our research questions, we conducted an online survey about the attribution of security responsibilities and trust in service providers with 170 participants. From our results, we identify an user mental model of distributed responsibility for online account security. There is a mismatch between this mental model and the stated privacy/security policies of service providers. We also find that *trust cues* seem to apply differently across SPs with different service offerings.

II. Background

Online user accounts are means by which users can access or benefit from an online service. Service providers (SPs) are the entities or corporations that provide these services, such as banks, shopping marketplaces, email providers, and social networking websites. Users provide personal information to their SP in order to use its services. The breadth and depth of personal information users provide depends on the type of service they are seeking. For example, a user wishing to buy or sell items through an online marketplace would have to provide her name, address and credit card number. SPs also collect information that users exchange through their service and information about how users utilize the service. These interactions necessarily require protective measures to ensure the security and privacy of user data.

It is unclear to what extent users and service providers are each responsible for protecting users' online accounts [7] [8]. Service providers expect users to take the security and privacy precautions described in their terms of use [9]. However, the terms of use change often, can be difficult to comprehend [10], and can be difficult to implement [11].

Nadon *et al.* [9] found that users are frustrated with "unrealistic responsibilities of acquiring encyclopaedist knowledge, in order to engage in informed consent." McDonald and Cranor [10] estimate that typical users would need 201 hours every year to fully read and understand their end-user license agreements (EULAs), based on the estimate that people visit 112 unique websites per month. Without proper understanding of EULAs, it is difficult for users to know who is responsible for which parts of their account security.

To begin to understand how users allocate responsibility for their security, Shay *et al.* [12] conducted a survey. They found that most participants either attributed responsibility to themselves (37%), or shared the responsibility with the service provider for preventing account compromises (40%), regardless of whether they had experienced an account compromise. Shay *et al.* take this as a favourable pretext for system design, and suggest that these results signify that a major barrier to adopting security tools – user attitudes – may be overcome. We aim to further the understanding of how users understand the responsibility of their security as it would be beneficial for usable security literature.

Additionally, in circumstances where users hold service providers responsible for their account security, what motivates them to trust that SPs will protect their private information?

The notion of trust is "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" [13]. Mayer and Schoorman [13] identify three beliefs about an entity which result in people trusting it: ability, integrity, and benevolence. Ability is the belief that the entity possesses the skills necessary to perform the service or function it claims. Integrity is the entity's compliance with its promises. Benevolence is the entity's goodwill towards others. When it comes to online service providers, people can hold one or two beliefs [14] about a particular service provider, or simultaneously hold all three beliefs [15].

Online service providers can facilitate trust from their users through several practices. They can provide users with control over their data [16]. Service providers can be transparent about their privacy and security policies by specifying their data handling practices and making it easy for users to locate and understand their policies [17]. Furthermore, specifying responsibility can promote user trust because it becomes clear to them which parts of the social contract their service provider is taking responsibility for and which parts are their responsibility [17].

To arrive at a belief about a service provider's trustworthiness, people use different *trust cues*. One common cue is *reputation*: "an assessment based on the history of interactions with or observations of an entity, either directly with the evaluator (personal experience) or as reported by others (recommendations or third party verification)" [18]. A service provider's good reputation can perhaps indicate integrity. Another cue for deriving trust is *visual design*. A website with a complex, busy layout, or in contrast, a bland design can indicate a lack of competence to some user groups [19], [20]. Similarly, a weak security/privacy statement [14] or unclear data handling policies [16] on a website can indicate a lack of benevolence.

Trust cues are not limited to those discussed here, and can take different forms. In our survey, we ask participants about trust cues that indicate competence and integrity. We discuss the findings of our survey and users' perceptions of responsibility within the context of SPs, a topic that has not yet been not deeply explored.

III. Methodology

This study was reviewed and cleared by our Institutional Research Ethics Board. We collected the data in June 2018. Our between-subjects online survey had 170 participants.

Each participant was placed in one of two groups, Facebook or Google, based on the screening question asking which account they use most regularly: Facebook, Google/Gmail, or both. Participants who used both accounts could be placed in either group. Ninety-five participants were assigned to the Facebook group and 75 to the Google group. Each group was asked questions relating to their respective platform (Facebook or Google). We hired Qualtrics to recruit participants and load balance. In all, 93 users reported having both Facebook and Google accounts. We asked Qualtrics for an even distribution, but their algorithm allocated more of these users to Facebook. This skew was increased when we removed responses that did not pass the integrity checks.

A. Survey

To help control for the integrity of the responses, we set a minimum time of 6 and a half minutes for participants to complete the survey. They were allowed to use as much time as they wanted beyond that. Participants took between 6 and a half minutes to 34 minutes to complete the survey, and the average time was 12 and a half minutes. To avoid response changes based on priming from later questions, once participants progressed through a page of questions they could not go back to a previous page,

We formulated a survey of 41 questions to reveal differences in user attitudes regarding account security and responsibility. The survey consisted of the following components: 1 screening question, 6 demographic questions (3 open-ended and 3 close-ended questions), and 35 security questions about: existing account monitoring practices and attitudes, opinions on the entities responsible for their account security, how they would like their service provider to monitor their account, the reasons they trust their service provider, and whether they believe that the service provider pertaining to their group is able to maintain the security of their data. Of the 35 security questions, there were 22 Likert scales, 4 open-ended, and 9 close-ended.

Individual questions are described in Section IV with their accompanying results. To test the survey, we conducted two iterations of pilot testing. The first iteration ($N = 5$) revealed that the meaning of some questions was confusing. We implemented improvements and ran a second pilot test ($N = 5$). We made some further minor wording tweaks, and removed a few questions to shorten the survey.

B. *Participants*

The majority of participants were recruited by Qualtrics. We paid Qualtrics $5.67 CAD per participant. From this, participants received reward points and monetary compensation from Qualtrics for completing the survey. Our own social media recruitment efforts yielded 6 responses; these participants did not receive compensation. In combination, we initially collected a total of 196 responses.

We excluded 26 participants because they picked the same Likert response in the entire survey, answered open-ended questions with non-words or non-English, did not follow our instructions to write *"no comment"* when they did not have an answer, or failed our quality-check question. Our quality-check question was designed to test attention: *What account is this survey about?* Participants could pick from six choices, including *Facebook* and *Google/Gmail*. The order of the choices was randomized. This resulted in 170 valid responses.

Half of the participants were female. Their ages ranged from 18 to 83 years old, with a mean age of 48, $SD = 15$ years. Thirty-nine of 170 were technical users based on their responses to the question, *Do you, or have you ever worked in a computer, computer security, or information technology (IT)-related field?*

IV. Results

In this paper, we focus our analysis on the 26 survey questions relating to RQ1 and RQ2.

A. *RQ1: Attribution of Responsibility*

Participants identified clear roles for themselves and their service providers with respect to the proactive and reactive security measures provided.

We asked participants about 10 *responsibility items*. Each participant, regardless of group, provided two Likert scale responses out of 5 for each item: one response for themselves, and one for the service provider (SP). Median scores, mean Likert scores, and standard deviations are listed in Table I. In all cases, higher scores indicate the attribution of more responsibility.

To determine whether there are significant differences between the two entities (*i.e.*, user and service provider) in how participants allocated responsibility, we performed 10 Wilcoxon signed rank tests using IBM SPSS. To control for familywise error, we applied a Bonferroni correction [21]. Table II lists the results of the Wilcoxon signed rank tests, with significant results in bold. We found that the distribution of responsibility was significantly different between the two entities (users v.s. SP) for 7 out of the 10 *responsibility items*. Figure 1 shows a high-level summary of the results. There was no effect of group (Facebook v.s. Google) on how participants allocated responsibility for the items. Both Facebook and Google participants allocated responsibility the same way[1].

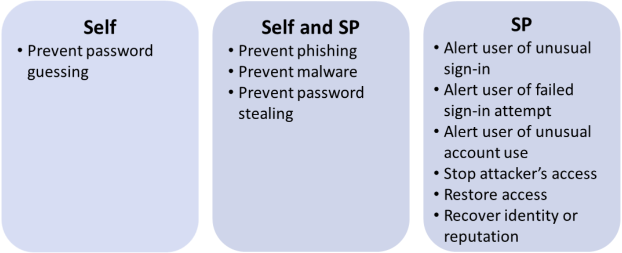
Self
• Prevent password guessing
Self and SP
• Prevent phishing
• Prevent malware
• Prevent password stealing
SP
• Alert user of unusual sign-in
• Alert user of failed sign-in attempt
• Alert user of unusual account use
• Stop attacker's access
• Restore access
• Recover identity or reputation

Fig. 1. Participants' attribution of primary responsibility for their account security.

1) *Do users allocate responsibility to any other entities?:* We asked participants to list any other entities responsible for prevention, alerting, and recovery. Only 13 of 170 provided a third entity. Except where otherwise listed, each answer was mentioned by only one participant. Facebook participants identified their friends, mobile device, email provider, third-party accounts linked to Facebook, antivirus program ($n = 2$), and browser. Google participants mentioned other software, antivirus program, third-party accounts linked to Google, and the government ($n = 3$).

B. *RQ2: Trust in Service Providers*

Our aim was not to directly compare the two SPs against each other. However, we found that participants trust Facebook and Google for different reason. We explore these differences further in this section.

Overall, Google participants were more likely to select *they have a good reputation*. Google participants rated their SP's ability to keep their data safe significantly higher than Facebook. Participants from the Facebook group were significantly more concerned about the security of their accounts. The leading reason for participants in both groups that would cause them to delete their accounts is a lack of protection from their service provider or their account being compromised.

1) *What makes [SP] trustworthy? Check all that apply.:* For this close-ended question, we provided 10 choices (*i.e., trust cues*), plus the option to define their own reason. Participants could pick more than one item. Figure 2 shows the percentage of participants who picked each trust cue. Overall, Google received a higher percentage of selections in all trust cues

[1] Results of non-significant group effect statistics are excluded from this paper for brevity.

TABLE I
MEDIAN LIKERT SCORE, MEAN LIKERT SCORE (STANDARD DEVIATION) OF PARTICIPANTS' ALLOCATION OF RESPONSIBILITY TO THEIR SP AND THEMSELVES, BY GROUP, AND OVERALL. SIGNIFICANTLY DIFFERENT PAIRS ARE BOLDED.

To what extent do you believe [SP is/you are] responsible for:	Facebook				Google				All			
	SP		Self		SP		Self		SP		Self	
	MD	M (SD)	MD	M (SD)	MD	M (SD)	MD	M (SD)	MD	M (SD)	MD	M (SD)
Preventing you from falling victim to a phishing attack?	4	3.8 (1.2)	4	3.8 (1.2)	4	3.6 (1.1)	4	4.0 (0.9)	4	3.7 (1.2)	4	3.9 (1.1)
Preventing your data or devices from getting infected with malware through your account?	5	4.1 (1.2)	4	3.8 (1.2)	4	3.9 (1.1)	4	3.9 (0.9)	4	4.0 (1.2)	4	3.8 (1.1)
Preventing your password from being stolen (being hacked)?	4	4.1 (1.2)	4	3.8 (1.2)	4	4.0 (1.0)	4	3.7 (1.0)	4	4.0 (1.1)	4	3.7 (1.1)
Preventing your password from being guessed by an attacker?	4	3.5 (1.3)	4	3.9 (1.1)	4	3.4 (1.4)	4	4.0 (1.0)	**4**	**3.4 (1.3)**	**4**	**4.0 (1.0)**
Alerting you or reporting to SP of a sign-in that is not from you?	5	4.5 (0.8)	4	3.6 (1.3)	5	4.6 (0.6)	4	3.8 (1.2)	**5**	**4.5 (0.7)**	**4**	**3.7 (1.2)**
Alerting you or reporting to SP of a failed sign-in attempt not from you?	5	4.6 (0.6)	4	3.5 (1.3)	5	4.5 (0.7)	4	3.7 (1.3)	**5**	**4.5 (0.7)**	**4**	**3.6 (1.3)**
Alerting you or reporting to SP of account use not from you?	5	4.4 (0.7)	4	3.7 (1.3)	4	4.4 (0.7)	4	3.6 (1.2)	**5**	**4.4 (0.7)**	**4**	**3.7 (1.2)**
Stopping the attacker's access to your account?	5	4.5 (0.7)	4	3.1 (1.2)	4	4.4 (0.7)	4	3.6 (1.1)	**5**	**4.4 (0.7)**	**4**	**3.3 (1.2)**
Restoring rightful access to your account?	5	4.6 (0.7)	4	3.0 (1.3)	5	4.4 (0.8)	4	3.4 (1.0)	**5**	**4.5 (0.8)**	**4**	**3.2 (1.2)**
Recovering your identity or reputation after an attack?	4	4.2 (1.0)	4	3.3 (1.3)	4	4.1 (0.9)	4	3.6 (1.1)	**4**	**4.2 (1.0)**	**4**	**3.4 (1.3)**

TABLE II
WILCOXON SIGNED RANK TEST COMPARING THE ATTRIBUTION OF RESPONSIBILITY BETWEEN THE TWO ENTITIES (USERS AND SPS). SIGNIFICANT RESULTS ARE BOLDED.

Responsibility item	Result		
Prevent phishing	$T = 3,338$	$p = .217$	$r = .09$
Prevent malware	$T = 2,073.50$	$p = .152$	$r = -0.11$
Prevent password stealing	$T = 1,743.50$	$p = .030$	$r = -0.17$
Prevent password guessing	**T = 3,618**	**p < .001**	**r = .27**
Alert/report unusual sign-in	**T = 384**	**p < .001**	**r = -.53**
Alert/report failed sign-in	**T = 336.5**	**p < .001**	**r = -.59**
Alert/report unusual account use	**T = 828**	**p < .001**	**r = -.49**
Stop attacker's access	**T = 574**	**p < .001**	**r = -.60**
Restore access	**T = 480**	**p < .001**	**r = -.68**
Restore identity / reputation	**T = 1,617**	**p < .001**	**r = -.37**

except for one, *many people have accounts with them*, in which Facebook received 2% more of the group total than Google.

Eighteen participants in the Facebook group provided written responses to the *Other* option. They believed that Facebook is not trustworthy (9), were unsure of Facebook's trustworthiness (4), and indicated that their trust in Facebook is declining (1). One participant indicated that none of the choices apply to Facebook. The remaining three comments were, *"no," "no comment,"* and *"Need to protect their reputation."* Only one participant in the Google group indicated that they do not trust Google.

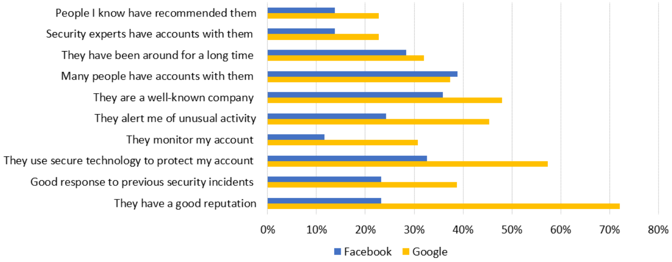

Fig. 2. Percentage of participants in each group responding to, *What makes each service provider trustworthy?* Multiple responses allowed.

2) [Facebook/Google] is able to keep my data safe.: We used a 5-point Likert scale for this question, asking participants to indicate their level of agreement or disagreement with this statement. 55% of Facebook (*Mean Likert score* = 3.38, *SD* = 1.04, *Median* = 4.00) participants and 89% of Google participants (*Mean Likert score* = 4.16, *SD* = 0.74, *Median* = 4.00) selected *somewhat agree* or *strongly agree*. A Mann-Whitney test found a significant difference between the two groups, $U = 5,121$, $z = 5.30$, $p < .001$, $r = .41$. Google participants rated their SP's ability to keep their data safe significantly higher than Facebook.

3) How concerned are you about the security of your [Facebook/Google] account?: We used a 5-point Likert scale for this question. 67% of Facebook participants (*Mean Likert score* = 3.79, *SD* = 0.93, *Median* = 4.00) and 57% of Google participants (*Mean Likert score* = 3.45, *SD* = 1.07, *Median* = 4.00) selected *somewhat concerned* or *extremely concerned*. A Mann-Whitney test found that participants from the Facebook group were significantly more concerned about the security of

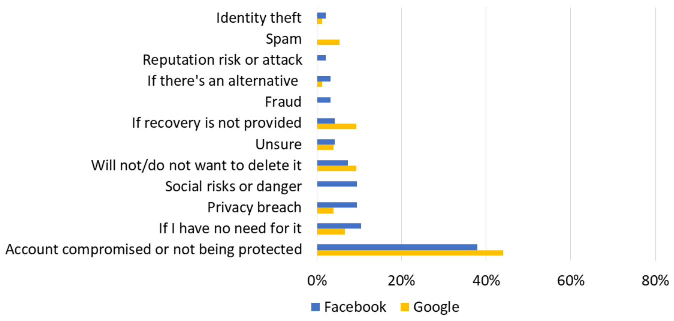

Fig. 3. Percentage of participants in each group providing reasons why they would delete their account. Multiple responses allowed.

their accounts than the Google group, $U = 2,968$, $z = -1.98$, $p = .048$, $r = -0.15$. We speculate that the higher concern for security is a result of recent media coverage on third-party access to Facebook users' data [22].

4) What would lead you to delete your [Facebook/Google] account?: This was an open-ended question. Using thematic analysis techniques, one researcher organized participants' answers into 12 emerging categories based on similarity. These categories are depicted in Figure 3 where the percentages represent the total number of survey respondents within each group (Google or Facebook). Some participants provided more than one reason, and a few did not provide any. The top reason in both groups was compromise or lack of protection for their accounts. Only Facebook participants were concerned with risks to reputation (2%), fraud (3%) and social dangers (10%), while only Google participants were concerned with spam (5%). The risks mentioned by participants seem to align with the service offerings of each service providers.

V. Discussion

In this paper, we have two purposes. First, we reveal which security measures users hold themselves responsible for, which measures they believe they share responsibility with their service provider, and which measures they believe their service provider is primarily responsible to take. Second, we suggest which factors motivate users to trust their service providers to maintain their security and thus take on a passive role in security management.

Our key findings suggest that users are not taking particular measures that are needed to maintain their online security and privacy because they do not hold themselves responsible for such or, they believe they share the responsibility their service provider but "sharing" is vaguely understood. We discuss these key findings and potential implications further below.

A. RQ1: Attribution of Responsibility

Participants attributed primary responsibility to the service provider for all reactive security measures, shared responsibility for most proactive measures, and took primary responsibility for preventing password guessing attacks, as depicted in Figure 1. A possible explanation for this distribution of responsibility is that users have control over maintaining strong passwords to prevent password guessing attacks, and have been taught how to engage with this protection strategy. On the other hand, they may not be able to, or know how to, recover their accounts or identities. Similarly, users must largely rely on user interface cues to detect threats to their accounts, so it makes sense for them to attribute primary responsibility to service providers to alert them of unusual activity. This implies that agency plays an important role in how users perceive responsibility. If users had more agency over reactive security measures, would those measures shift over to the shared category (*Self and SP* in Figure 1)?

Our findings on responsibility indicate a mismatch between user and service provider expectations. Users' mental model of how responsibility is distributed between themselves and their SP does not align with the SPs' allocated roles.

Facebook's terms of service state, *"We make no guarantees that [our products] always will be safe, secure, or error-free [...] Under no circumstance will we be liable to you for any lost profits, revenues, information, or data, or consequential, special, indirect, exemplary, punitive, or incidental damages [...] even if we have been advised of the possibility of such damages"* [23]. Google's terms of service state, *"Google [...] will not be responsible for lost profits, revenues, or data, financial losses or indirect, special, consequential, exemplary, or punitive damages"* [24]. We chose Facebook and Google due to their popularity, but this mismatch in expectations extends to other SPs as well [11], [25]. This implies a need for user education about EULAs. A possible design implication is that security decision support tools can be leveraged to highlight to users the most consequential security policies in the EULAs, based on their practices and attitudes. For example, a security decision support tool can highlight to an avid social media user the possible consequences of sharing personally identifiable information (*e.g.*, identity theft) and the user's corresponding responsibility in the event of an incident (*e.g.*, to recover one's identity). These tools could operate in the same way as proposed privacy decision support tools [25].

B. RQ2: Trust in Service Providers

Both Facebook and Google users trust their SP for a variety of reasons, but Google users were much more likely to trust their SP based on its reputation. Facebook users were more concerned about their account security and less confident in their SP's ability to keep their data safe. The top reason that would cause both Facebook and Google participants to delete their accounts is a perceived lack of protection from their service provider and/or their accounts being compromised. These findings suggest that service providers should consider the trust cues most relevant to their service offerings when evaluating their products.

We speculate that the recent privacy breach by a third-party app on Facebook [22] played a role in its lower trust ratings. One participant commented *"I should actually delete [my account] with all the information that's come out in recent months"*. Another participant indicated, *"Unsure, however I have debated deleting it after recent security issues that have* *been exposed"*. Despite these attitudes, the top two trust cues that Facebook participants selected were *many people have accounts with them* and *they are a well-known company.* This suggests that longevity and popularity are powerful reasons for people to trust a service provider enough to use it. Other social factors could also be at play. For example, the wide usage of a platform could motivate people to join it to avoid being isolated, or simply because there is no viable alternative [25]–[28].

Per this study's limitations, our survey was mostly accessible to online survey respondents through the Qualtrics platform. Online surveys provide access to a wider population, yet they may suffer from self-reporting bias and sampling bias [29]. Furthermore, while our results cover two main service providers, further work would be needed to confirm whether the findings hold across other providers.

VI. Conclusion

Respondents to our survey generally trust Facebook or Google to keep their account safe, yet there is a mismatch in expectations between users and service providers. Participants ascribed clear roles with respect to primary responsibility between themselves and their service provider for the security of their accounts. This division of labour, however, does not match the roles set out in service providers' EULAs and suggests that users have inaccurate mental models in this regard. We identify a potential for the design of security decision support tools to help users better manage their accounts. We suggest improved communication of EULAs to also help users form better mental models. When service providers expect users to play an active role in both proactive and reactive security measures, it becomes necessary to enable user agency by making such measures (*e.g.*, account monitoring) usable and accessible. We also find that user trust differed between SPs with different service offerings, suggesting that one-size-fits-all approaches are unlikely to be successful. We caution against over generalizing research relating to trust and security across domains.

VII. Acknowledgements

We thank our reviewers and participants for their time. S. Chiasson acknowledges funding from NSERC for her Canada Research Chair and Discovery grants.

References

[1] A. Press, "Google defends its right to scan Gmail accounts as outraged privacy advocates seek to end practice," *Financial Post (online)*, 2013. [Online]. Available: https://business.financialpost.com/technology/google-gmail-scanning-privacy

[2] K. Granville, "Facebook and cambridge analytica: What you need to know as fallout widens," https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html, 2018.

[3] Facebook Inc, "Company info," https://newsroom.fb.com/company-info/, 2018.

[4] L. Matney, "Google has 2 billion users on Android, 500M on Google photos," https://techcrunch.com/2017/05/17/google-has-2-billion-users-on-android-500m-on-google-photos/, 2017.

[5] Miniwatts Marketing Group, "World internet users and 2018 population stats," https://www.internetworldstats.com/stats.htm, 2018.

[6] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki *et al.*, "Data breaches, phishing, or malware?: Understanding the risks of stolen credentials," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 1421–1434.

[7] J. Simon, *Distributed epistemic responsibility in a hyperconnected era*. Springer, 2015, pp. 145–159.

[8] J. Simon and I. Shklovski, "Lessening the burden of individualized responsibility in the socio-technical world," *Proceedings of ISIS Summit-The Information Society at the Crossroads*, pp. 1–5, 2015.

[9] G. Nadon, M. Feilberg, M. Johansen, and I. Shklovski, "In the user we trust: Unrealistic expectations of Facebook's privacy mechanisms," in *Proceedings of the 9th International Conference on Social Media and Society*. ACM, 2018, pp. 138–149.

[10] A. M. McDonald and L. F. Cranor, "The cost of reading privacy policies," *ISJLP*, vol. 4, p. 543, 2008.

[11] M. Mannan and P. C. van Oorschot, "Security and usability: the gap in real-world online banking," in *Proceedings of the 2007 Workshop on New Security Paradigms*. ACM, 2008, pp. 1–14.

[12] R. Shay, I. Ion, R. W. Reeder, and S. Consolvo, "My religious aunt asked why I was trying to sell her viagra: experiences with account hijacking," in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014, pp. 2657–2666.

[13] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of management review*, vol. 20, no. 3, pp. 709–734, 1995.

[14] A. E. Schlosser, T. B. White, and S. M. Lloyd, "Converting web site visitors into buyers: how web site investment increases consumer trusting beliefs and online purchase intentions," *Journal of Marketing*, vol. 70, no. 2, pp. 133–148, 2006.

[15] D. Gefen, "Reflections on the dimensions of trust and trustworthiness among online consumers," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, vol. 33, no. 3, pp. 38–53, 2002.

[16] K. M. Khan and Q. Malluhi, "Establishing trust in cloud computing," *IT professional*, no. 5, pp. 20–27, 2010.

[17] B. Shneiderman, "Designing trust into online experiences," *Communications of the ACM*, vol. 43, no. 12, pp. 57–59, 2000.

[18] D. Artz and Y. Gil, "A survey of trust in computer science and the semantic web," *Web Semantics: Science, Services and Agents on the World Wide Web*, vol. 5, no. 2, pp. 58–71, 2007.

[19] E. Sillence, P. Briggs, L. Fishwick, and P. Harris, "Trust and mistrust of online health sites," in *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 2004, pp. 663–670.

[20] R. T. Stephens, "A framework for the identification of electronic commerce design elements that enable trust within the small hotel industry," in *Proceedings of the 42nd annual Southeast regional conference*. ACM, 2004, pp. 309–314.

[21] A. Field, *Discovering statistics using IBM SPSS statistics*. sage, 2013.

[22] Facebook Inc., "An update on our plans to restrict data access on Facebook," https://newsroom.fb.com/news/2018/04/restricting-data-access/, 2018.

[23] Facebook Inc, "Terms of service," https://www.facebook.com/legal/terms, 2018.

[24] Google, "Terms of service," https://policies.google.com/terms, 2018.

[25] A. Rao, F. Schaub, N. Sadeh, A. Acquisti, and R. Kang, "Expecting the unexpected: Understanding mismatched privacy expectations online," in *Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2016.

[26] A. Hakkala, O. I. Heimo, S. Hyrynsalmi, and K. K. Kimppa, "Security, privacy'); drop table users;-and forced trust in the information age?: when trusting an information system is not optional and why it matters," *ACM SIGCAS Computers and Society*, vol. 47, no. 4, pp. 68–80, 2018.

[27] S. Stieger, C. Burger, M. Bohn, and M. Voracek, "Who commits virtual identity suicide? Differences in privacy concerns, internet addiction, and personality between facebook users and quitters," *Cyberpsychology, Behavior, and Social Networking*, vol. 16, no. 9, pp. 629–634, 2013.

[28] E. P. Baumer, P. Adams, V. D. Khovanskaya, T. C. Liao, M. E. Smith, V. Schwanda Sosik, and K. Williams, "Limiting, leaving, and (re) lapsing: an exploration of facebook non-use practices and experiences," in *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM, 2013, pp. 3257–3266.

[29] E. M. Redmiles, Y. Acar, S. Fahl, and M. L. Mazurek, "A summary of survey methodology best practices for security and privacy researchers," Technical Reports of the Computer Science Department, University of Maryland, Tech. Rep., 2017.