Privacy Policy Analysis and Verification of Messaging Applications

Matthew Pudlo
North Carolina State University
Raleigh, North Carolina, USA
mrpudlo@ncsu.edu

Corey Capooci
North Carolina State University
cvcapooc@ncsu.edu

Brooke Loudermilk
North Carolina State University
blouder@ncsu.edu

ABSTRACT

This study, tested two popular messaging applications, Slack and Discord, to see if the content of messages exchanged by users could be used to profile those users for advertising purposes. The study exchanged topical messages between pairs of users, and in a group chat situation, over a period of three weeks. Testers periodically recorded the advertisements shown to each user when web browsing to common websites. This was able to show that the percentage of those ads that were related to the topics of conversation, while small, increased by two to three times over the course of the three weeks. It would be interesting to continue the study over a longer period of time, and with additional applications, for further investigation and analysis.

CCS CONCEPTS

• **Security and Privacy** → *Privacy Protections*; *Economics of security and privacy*.

KEYWORDS

privacy policy, messaging applications

ACM Reference Format:
Matthew Pudlo, Corey Capooci, and Brooke Loudermilk. 2018. Privacy Policy Analysis and Verification of Messaging Applications. In *Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

The increase in usage of messaging applications, particular on mobile devices, has increased exponentially over the past decade or so. This growth has been catalyzed by the global COVID-19 pandemic in many cases, as communication via messaging (including video chat) applications became, for many, their only means of interacting with friends, family, and co-workers. From 2012 to 2021, the number of active users claimed by WeChat grew from 50 million to 1.24 billion. WhatsApp reported growth in monthly active users from 10 million in late 2010, to 2 billion in early 2021. The relative newness of such applications, when compared to the Internet as a whole, means that many or most users are more naive about privacy and security concerns related to such application usage when compared to traditional internet browsing. Additionally, the large number of messaging applications makes it likely that much privacy policies and privacy behaviors of such apps vary greatly, and makes verification of privacy policy truthfulness more difficult.

Several recent controversies spurred our interest in this topic. When Zoom's popularity skyrocketed in 2020 as a result of the global COVID-19 pandemic, it came under fire for having invalidly claimed to provide end-to-end encryption. In early 2021, WhatsApp pushed out notifications to its users telling them that they would have to accept WhatsApp policy changes in order to keep using the application. Users were scared off both by the belief that WhatsApp would be collecting additional user information and content, and by the fact that the change was mandatory and on short notice.

Woodstock '18, June 03–05, 2018, Woodstock, NY
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

Some people abandoned WhatsApp in favor of other messaging applications with stronger privacy claims, such as Signal and Telegram.

This study attempted to determine whether two of these popular messaging applications, Slack and Discord, are more invasive of their user's privacy than their privacy policies convey. Slack's privacy policy states that they collect user metadata, and that they may share aggregated or de-identified data with third parties. The policy implies that this statement is in reference to metadata, but the policy is vague. The Discord privacy policy similarly states that they may collect and share "aggregated or non-identifiable data", but does not enumerate what the types or source of this data might be. As there is not a standard language or representation used by companies in writing privacy policies, the details of the policies are open to interpretation.

2 APPROACH

The goal of the study was to isolate chat data as a source of targeted advertisements. The experiment was designed to mimic real life user interaction. To preform the experiment eight fake user profiles were created and each assigned to an identical copy of a virtual machine using the Ubuntu OS. Each of the virtual machines were hosted on the same computer in one fixed location.

As each of the users, a tester would use chrome with no ad blocker or other extensions, to browse a set of four test websites: cnn.com, msncb.com, reddit.com, wral.com. The tester manually recorded each of the advertisement presented to the user. This initial collection served as a baseline for comparing how advertisements changed for users.

Each of the fake users was then separated into two groups and each group was assigned a different platform to have conversations on. Users 1 through 4 were assigned to use slack and Users 5 through 8 were assigned to have the conversations on Discord. Twice a week each group of users would have 4 one on one conversations and one group chat amongst all four members. The conversation topics were assigned as follows:

Football: Users 1 and 2, Users 5 and 6
Kayaking: Users 2 and 3, Users 6 and 7
Jewelry: Users 3 and 4, Users 7 and 8
Dogs: Users 4 and 1, Users 8 and 5
Cooking: Users 1 through 4, Users 5 through 8

Table 1: Baseline Categorization

User	Total	On	Other	Group
1	36	0	0	0
2	41	2	0	0
3	38	1	2	0
4	40	1	1	1
5	39	3	0	1
6	40	0	0	0
7	36	0	1	0
8	39	0	0	0

After each week of conversations, a tester would revisit the home pages of the set of test websites. The tester would then manually record of the advertisements presented to the user and use this data to compare how ads changed from the baseline of each user. The process of having two conversations and recording advertisements was repeated for three weeks.

To reduce error in the experiment each individual conversation about a topic was identical despite what platform the user was on. For example, every conversation on football between users one and two was repeated exactly with users 5 and 6. The only websites that any of the users visited in the virtual machine was the set of four test websites. No tester clicked on any ad or followed links off the homepage. The only activity on the virtual machines was creating the user accounts, recording information off of test websites, and having chats between users. The virtual machines were all created from the same image to reduce fingerprinting. Special consideration was made to not sign in or use any personal accounts on any of the VMs.

3 EVALUATION

Evaluation of the study was conducted by examining the frequency and categories of the advertisements across the different users. Each advertisement for a user was manually categorized into one of four categories: Related to User Topics, related to other User Topics[on], Related to Group Chat Topic[Group], or Unrelated[other]. Tables 1 through 4 display the results of this categorization as the experiment progressed through baseline to final collection.

Table 2: Week 1 Categorization

User	Total	On	Other	Group
1	35	1	6	1
2	38	2	2	0
3	43	1	2	0
4	40	2	2	1
5	38	1	5	0
6	39	0	2	0
7	36	1	0	0
8	36	2	0	1

Table 3: Week 2 Categorization

User	Total	On	Other	Group
1	32	2	2	1
2	41	2	5	1
3	37	1	1	1
4	41	7	3	1
5	37	1	5	0
6	42	1	3	0
7	41	3	1	0
8	39	1	0	1

Table 4: Week 3 Final Categorization

User	Total	On	Other	Group
1	36	3	5	0
2	48	3	3	2
3	36	3	3	0
4	39	0	4	0
5	42	4	1	0
6	43	3	1	0
7	36	2	0	0
8	38	2	3	1

Initially most of the advertisements viewed had little to do with the topics of conversations. Only a few relevant ads were presented in the baseline test. These can be attributed to being general topics and mainly presented themselves in related to football or pets. At the baseline the advertisements seemed to be targeting the general audience who would view the site or the general population. Many of the news sites presented advertisements on Finances, Banking, Technology, or Travel. As the weeks progressed we observed the patterns of advertisements changing for each user. The advertisements seemed to become more unique for each user after more chats have occurred.

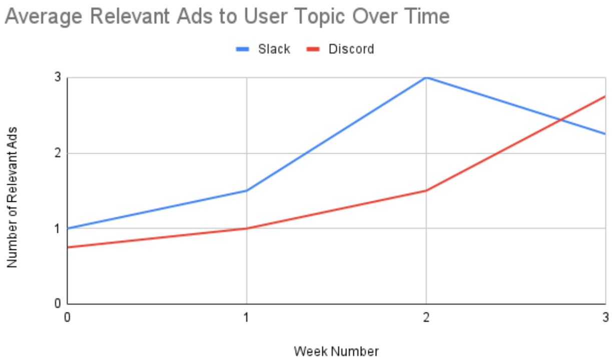

Figure 1: Related ads to users topic over time

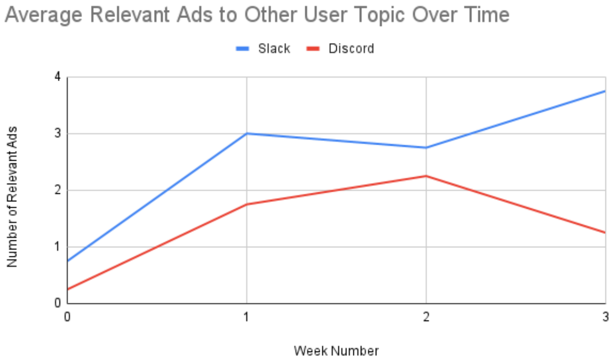

Figure 2: Related ads to other users topics over time

As the weeks progressed, more ads were seen targeted to a users topics. A small uptick in targeted advertising was seen after just one week but a much larger increase can be seen after the second week. An increase in advertisements related to other users topics was also observed. 87.5% of users saw an increase in advertisements related to their topics of conversation and the same percentage of users saw an increase in ad's related to other users topics as well. This indicates some crossover of information between the network of users chatting and some transitive assumptions that interconnected users may enjoy the same things.

Figures 1 and 2 show how the average number of relevant advertisements increased over time.

4 RELATED WORKS

Related works include research on privacy policies and research on techniques used in secure messaging and video applications. Secure messaging research focuses on the technical details to make end-to-end encryption work practically in protocols such as Signal. This leads to research in more specific applications such as end-to-end encryption of group messaging, which is different and arguably more difficult problem to solve. In addition, there is research regarding the mental model users have about end-to-end encryption. Furthermore, research on privacy policies and privacy statements centered around the effectiveness of privacy statements to convey their information. This includes analysis on the appropriate reading level of privacy policies and new designs of the privacy policy in order to make it more accessible to a wider audience.

Works related to messaging application and end-to-end encryption focus on implementation, analysis, and improvements upon previous iterations. Recent work analyzes and addresses flaws in end-to-end encryption applications such as post compromise security in relation to clone detection, statistical disclosure attacks especially associated with the sealed sender feature of the Signal messaging service, and abuse of contact discovery to leak relationship information [8, 13, 18]. Additional work traces the privacy and security improvements of newer smartphone messaging applications in comparison to older ones, but states that newer applications have much progress to make [19]. Other works continue to look at iterations of secure messaging protocols such as Signal and Off the Record Messaging and suggest modifications to improve the protocols [5, 22]. More works take a closer look at specific messaging applications such as Facebook Messenger and the implications on personal data privacy [20]. End-to-end encryption research encompasses many other areas of technology including email [24]. There is also research that analyzes privacy crises involving communication platforms such as Zoom [28] .

There is a lot of focus on providing private group messaging. The research topics around private group messaging include techniques for achieving privacy and the limitations of one-to-one end-to-end encryption when applying it to group conversations [15]. Messaging systems mentioned in writing include the Riposte, Mobile CoWPI, Dissent, and the Signal Private Group System [3, 4, 7, 23]. Each of the concepts have certain properties they attempt to hold in order to improve the privacy and security of group messaging protocols. There has also been research specifically related to guaranteeing the post-compromise security of the group messaging [6, 9].

The work in this experiment is supplemented by similar works in the area of the public mental model of end-to-end encryption and privacy policies. There is research on the perceived level of trust given to a website based on the handling of the user's data on that website [11]. This shows that accurate and understandable privacy statements can go a long way to help build public trust. Other work focuses on the mental model of end-to-end encryption such as the accuracy of the public's mental model, the improvement of the public's mental model when provided additional information involving end-to-end encryption, and the public's trust in secure messaging that uses end-to-end encryption.[1, 2, 10].

Research on privacy policies includes discussion on privacy policies in highly sensitive areas of technology, content analysis, layouts of privacy policies, and privacy policy processing. Some works dive into the privacy policies in areas such as internet of things, web platforms, and online banks applications since these areas contain highly valuable private information [14, 21, 25, 27]. In addition, other works focus on processing the privacy policies themselves. Works include content analysis of cloud computer privacy statements to understand what information is collected and where it goes [12]. There is also keyword analysis that helps determine the impacts of regulations on privacy statements [16]. Other work focuses on the automation of understanding privacy statements [26]. Other researchers work on creating standardized privacy statements to improve comprehension amongst readers [17]. More current high impact research focuses on the COVID tracking apps and their policies in order to improve their use and trust [29].

There has been no work directly related to privacy statements and policies of messaging and voice chat applications and their accuracy. This experiment attempts to understand the accuracy of popular video and messaging chat applications' privacy policies in order to determine how much trust can be put into these statements. All other work tended to focus on privacy policies of other areas of technology or on the implementations of the chat applications themselves.

5 DISCUSSION

The limitations of the experiment focused on resource limitations from time to hardware and the lack of options in chat applications. Time limitations may have prevented more information from propagating to advertisement companies. Resource limitations caused difficulties with efficiency and usability of the experiment. Lessons learned from these resource limitations could help future experiments be more successful. Chat choice limitations prevent the use of some of the most popular applications which prevented the experiment from having a broader impact.

Future work should focus on removing the limitations of this experiment to get better results. For example, increase the time frame of the experiment to allow more time for information to reach the advertisement companies. In addition, include as many chat applications as possible to get a broad view of how the industry values their own privacy policies. Future work should target video chat applications as well.

One limitation was the inability to choose some of the most popular and widely used chat applications, such as Signal, Telegram, and Google Chat. Signal and Telegram require that all non-mobile users register with a mobile device with a phone number first. This experiment lacked the hardware to create four individual Telegram or Signal accounts for each of the users. This would have required four phones with different phone numbers. In addition, the phones and the phone number could not have been tied to any previous user. Any traces or links to a previous individual could taint the results of the experiment. Google Chat, on the other hand, or Google accounts all together had a similar resource requirement. Google accounts require the use of a phone number as well. Unlike Signal and Telegram, it did not require a mobile device with the app installed in order to link the computer's account and the mobile device's account. Instead, it used the phone number for a one time pin. Google recognized free online SMS phone numbers, so this provided a major roadblock in the use of the Google Chat application. Google continues to enhance their algorithms to ensure every user only acquires a fixed amount of accounts, so using Google Chat in the future should only get more and more difficult.

Even if it were easier to create user accounts for more chat applications, the necessary hardware resources for running a larger experiment would have surpassed those available for this experiment. In order to run an efficient and effective experiment, it would be best to be able to at least run all four users at once and type out their interactions one after another. In addition, additional hardware resources would allow data collection to be completed quicker and allowed for multiple virtual machines to be run at one time. The memory available, 8 GB, to this experiment made the process of chatting and data collection painstaking as at most two virtual machines were able to be run at once. It hampered the progress of the experiment and if the experiment were much larger the time spent chatting and collecting data would have been unmanageable. In addition, disk space was an issue as virtual machines could require upwards of 10GB of disk storage per machine especially for larger operating systems. This problem was fixed by using an external hard drive with enough available space.

Another resource constraint for this experiment was time. Since this experiment was limited to the course of a semester, the results of the experiment could be impacted by a short time frame between the first data collection and the last data collection. This experiment only spanned three weeks from the first collection to the last. This amount of time may not have allowed enough information from the chat conversations to be propagated to the advertisement companies.

To expand upon the results of this paper, future experiments should increase the number chat applications used in the experiment. Future experiments should analyze as many popular chat applications as possible. This may require obtaining many phones and phone numbers and enough hardware resources, such as RAM and disk space, to facilitate such an experiment, but it is worth broadening its scope to understand how the industry as a whole respects the contents of their privacy policy.

In addition to expanding the number of applications, it would be beneficial to expand the time frame of the experiment to ensure that any chat data that is being sold is properly accounted for in the advertisements. Like previously stated, a few weeks may not be enough time to see concrete advertisement outputs. It would be worth expanding the experiment to months to see the trend of increasing targeted advertisements regarding the discussion topics. This would provide data points such as which applications sell data, and how long it takes for the advertisements to start to appear.

Future experiments may also include using video chat applications. To create a more complete analysis of the chat application industry, it is beneficial to include video chat as well. This creates more problems to solve such as how to design and structure these conversations, but would also provide more interesting data on whether video chat applications have the ability the extract speech and sell that information.

This experiment's limitations include chat application choice, resource constraints, and time constraints. This resulted from difficulties in generating user accounts for different chat applications and from general time and resource constraints given a student-driven semester-long research project. The future work should remove some of these limitations by providing more time and hardware resources to complete this experiment. In addition, it should devise ways to create accounts across all of the chat applications including video chat application. Overall this may require access to additional mobile devices and mobile numbers.

6 CONCLUSION

The results gathered in this study seem to suggest that there is a correlation between the message content exchanged between users and the ads provided to those users at a later date when they use a standard browser to access common web sites that use targeted advertising. Additionally, there was a correlation between a particular user's chat topics and the targeted ads shown to a co-located (i.e, on the same sub-net) user with whom the original user had exchanged messages about a completely separate topic. While the overall percentage of ads related to user conversations remained very small after the three week study period, it was 2-3 times higher than the starting percentage of related ads, which had to have been shown by chance since the initial browsing was done before any conversations were executed.

The results suggest that it is possible that these chat applications are conducting analytics based not just on user metadata, but on user message content. This would be behavior that would violate the privacy policies of Slack and Discord, even if the message topics or content were never attributed to a specific user.

While a much larger sample size of conversations, collection dates, and specific applications would be necessary to draw any significant conclusions from the results of our study, our results were intriguing enough to feel that a larger study of this topic is warranted.

7 INDIVIDUAL CONTRIBUTIONS

Corey Capooci: Conducted privacy policy research on Signal and Telegram even though the applications were not chosen for the experiment. Wrote the Related works and Discussion sections of this paper. In addition, I built experiment setup by constructing VMs, creating user accounts, conducting twice weekly conversations written by teammates, and conducting weekly data collection. For presentation, I presented the slides, Limitations/Future Work and Design/Approach, that I created.

Brooke Loudermilk: I researched the privacy policies for Slack and other messaging applications. I contributed ideas to the design of the experiment setup, and attempted to help find workarounds for account creation issues. I wrote the content of the bi-weekly user conversations. I presented several slides on the final presentation. I wrote the Abstract, Introduction, and Conclusion for this paper.

Matthew Pudlo: Researched privacy policies for whats app and other messaging applications. Worked to create the experiment procedure and ensure external factors were sufficiently controlled for. Manually categorized the results of advertisement data collection. Preformed data analysis and analytics to generate results of study.

REFERENCES

[1] Ruba Abu-Salma, Elissa M. Redmiles, Blase Ur, and Miranda Wei. 2018. Exploring user mental models of end-to-end encrypted communication tools. *8th USENIX Workshop on Free and Open Communications on the Internet, FOCI 2018, co-located with USENIX Security 2018* (2018).

[2] Omer Akgul, Wei Bai, Shruti Das, and Michelle L Mazurek. [n.d.]. Evaluating In-Workflow Messages for Improving Mental Models of End-to-End Encryption. ([n. d.]). https://www.usenix.org/conference/usenixsecurity21/presentation/akgul

[3] Alex Arriaga, Peter D. Hart, Mark Jurkowitz, Geneva Overholser, and Robert Siegel. 2003. Dissent. *The Media and the War on Terrorism* (2003), 145–159. https://doi.org/10.5149/9780807872802_zeitz.6

[4] Melissa Chase, Trevor Perrin, and Greg Zaverucha. 2020. The Signal Private Group System and Anonymous Credentials Supporting Efficient Verifiable Encryption. In *Proceedings of the ACM Conference on Computer and Communications Security*. Association for Computing Machinery, 1445–1459. https://doi.org/10.1145/3372297.3417887

[5] Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila. 2020. A Formal Security Analysis

of the Signal Messaging Protocol. *Journal of Cryptology* 33, 4 (2020), 1914–1983. https://doi.org/10.1007/s00145-020-09360-1

[6] Katriel Cohn-Gordon, Cas Cremers, Luke Garratt, Jon Millican, and Kevin Milner. 2018. On Ends-to-Ends Encryption. (2018), 1802–1819. https://doi.org/10.1145/3243734.3243747

[7] Henry Corrigan-Gibbs, Dan Boneh, and David Mazières. 2015. Riposte: An anonymous messaging system handling millions of users. *Proceedings - IEEE Symposium on Security and Privacy* 2015-July (2015), 321–338. https://doi.org/10.1109/SP.2015.27 arXiv:1503.06115

[8] Cas Cremers, Jaiden Fairoze, Benjamin Kiesl, and Aurora Naska. 2020. Clone Detection in Secure Messaging: Improving Post-Compromise Security in Practice. *Proceedings of the ACM Conference on Computer and Communications Security* (2020), 1481–1495. https://doi.org/10.1145/3372297.3423354

[9] Cas Cremers, Britta Hale, and Konrad Kohbrok. [n.d.]. The Complexities of Healing in Secure Group Messaging: Why Cross-Group Effects Matter. ([n. d.]). https://www.usenix.org/conference/usenixsecurity21/presentation/cremers

[10] Sergej Dechand, Alena Naiakshina, Anastasia Danilova, and Matthew Smith. 2019. In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception. *Proceedings - 4th IEEE European Symposium on Security and Privacy, EURO S and P 2019* (2019), 401–415. https://doi.org/10.1109/EuroSP.2019.00037

[11] Carlos Flavián and Miguel Guinalíu. 2006. Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Industrial Management Data Systems* 106, 5 (2006), 601–620. https://doi.org/10.1108/02635570610666403

[12] Lei Gao and Alisa G. Brink. 2019. A content analysis of the privacy policies of cloud computing services. *Journal of Information Systems* 33, 3 (2019), 93–115. https://doi.org/10.2308/isys-52188

[13] Christoph Hagen, Christian Weinert, Christoph Sendner, Alexandra Dmitrienko, and Thomas Schneider. [n.d.]. All the Numbers are US: Large-scale Abuse of Contact Discovery in Mobile Messengers. ([n. d.]). https://doi.org/10.14722/ndss.2021.23159

[14] Yousra Javed, Elham Al Qahtani, and Mohamed Shehab. 2021. Privacy policy analysis of banks and mobile money services in the middle east. *Future Internet* 13, 1 (jan 2021), 1–15. https://doi.org/10.3390/FI13010010

[15] Christian Mainka. J¨org Schwenk Rosler Paul. 2018. On the End-to-End Security of Group Chats in Instant Messaging Protocols. *Proceedings of 3rd IEEE European Symposium on Security and Privacy (EuroSP 2018)* (2018).

[16] Jasmin Kaur, Rozita A. Dara, Charlie Obimbo, Fei Song, and Karen Menard. 2018. A comprehensive keyword analysis of online privacy policies. *Information Security Journal* 27, 5-6 (2018), 260–275. https://doi.org/10.1080/19393555.2019.1606368

[17] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing privacy notices. (2010), 1573. https://doi.org/10.1145/1753326.1753561

[18] Ian Martiny, Gabriel Kaptchuk, Adam Aviv, Dan Roche, and Eric Wustrow. [n.d.]. Improving Signal's Sealed Sender. ([n. d.]). https://doi.org/10.14722/ndss.2021.23180

[19] Robin Mueller, Sebastian Schrittwieser, Peter Fruehwirt, Peter Kieseberg, and Edgar Weippl. 2015. Security and privacy of smartphone messaging applications. *International Journal of Pervasive Computing and Communications* 11, 2 (2015), 132–150. https://doi.org/10.1108/IJPCC-04-2015-0020

[20] Morris Ntonja and Moses Ashawa. 2020. Examining artifacts generated by setting Facebook Messenger as a default SMS application on Android: Implication for personal data privacy . *Security and Privacy* 3, 6 (nov 2020). https://doi.org/10.1002/SPY2.128

[21] Alfredo J. Perez, Sherali Zeadally, and Jonathan Cochran. 2018. A review and an empirical analysis of privacy policy and notices for consumer Internet of things. *Security and Privacy* 1, 3 (may 2018), e15. https://doi.org/10.1002/SPY2.15

[22] Mario Di Raimondo and Hugo Krawczyk. [n.d.]. Secure Off-the-Record Messaging. ([n. d.]), 81–89.

[23] Michael Schliep and Nicholas Hopper. 2019. End-to-end secure mobile group messaging with conversation integrity and deniability. *Proceedings of the ACM Conference on Computer and Communications Security* (2019), 55–73. https://doi.org/10.1145/3338498.3358644

[24] Jörg Schwenk, Marcus Brinkmann, Damian Poddebniak, Jens Müller, Juraj Somorovsky, and Sebastian Schinzel. 2020. Mitigation of Attacks on Email End-to-End Encryption. *Proceedings of the ACM Conference on Computer and Communications Security* (2020), 1647–1664. https://doi.org/10.1145/3372297.3417878

[25] Parvaneh Shayegh and Sepideh Ghanavati. 2017. Toward an approach to privacy notices in IoT. *Proceedings - 2017 IEEE 25th International Requirements Engineering Conference Workshops, REW 2017* (2017), 104–110. https://doi.org/10.1109/REW.2017.77

[26] Shomir Wilson, Florian Schaub, Aswarth Abhilash Dara, Frederick Liu, Sushain Cherivirala, Pedro Giovanni Leon, Mads Schaarup Andersen, Sebastian Zimmeck, Kanthashree Mysore Sathyendra, N. Cameron Russell, Thomas B. Norton, Eduard Hovy, Joel Reidenberg, and Norman Sadeh. 2016. The creation and analysis of a Website privacy policy corpus. *54th Annual Meeting of the Association for Computational Linguistics, ACL 2016 - Long Papers* 3 (2016), 1330–1340. https://doi.org/10.18653/v1/p16-1126

[27] Stephanie Winkler and Sherali Zeadally. 2016. Privacy Policy Analysis of Popular Web Platforms. *IEEE Technology and Society Magazine* 35, 2 (2016), 75–85. https://doi.org/10.1109/MTS.2016.2554419

[28] Sarah Young. 2021. Zoombombing Your Toddler: User Experience and the Communication of Zoom's Privacy Crisis. *Journal of Business and Technical Communication* 35, 1 (2021), 147–153. https://doi.org/10.1177/1050651920959201

[29] Melvyn Zhang, Aloysius Chow, and Helen Smith. 2020. COVID-19 contact-tracing apps: Analysis of the readability of privacy policies. *Journal of Medical Internet Research* 22, 12 (2020), 1–6. https://doi.org/10.2196/21572