A Real-World Evaluation of Privacy Nutrition Labels

Qilei Cai, Crystal Song, Andrew Weng

New York University, Computer Science & Engineering Dept.
CS9223 - Privacy in the Electronic Society
Spring 2022
{qc542, cs5489, aw4108}@nyu.edu

***Abstract* — As online services become increasingly prevalent in our day to day activities, privacy and knowledge of data collection practices are becoming increasingly important to the end user. However, despite their interest, users have been dissuaded and otherwise prevented from informing themselves in part due to the length and complexity of privacy policies. In an effort to mitigate this, Apple developed App Privacy Labels – their implementation of "Privacy Nutrition Labels". We conducted a survey to investigate the efficacy of this new feature. Our results showed that users considered the information on the labels to be valuable and in some cases altered their decision to download the app based on the information they were shown. We find App Privacy Labels to be effective, validate previous work with real-world findings, and propose directions for future research.**

I. Introduction

Nearly every online service requires users to acknowledge a collection of statements that describes how their personal data is used. Over the last two decades the efficacy and utility of these now-ubiquitous disclosures has been the topic of a lively research conversation, much of which suggests that privacy policies are too long, too complex, often contain irrelevant information, and are ultimately ineffective at conveying information and granting the power of choice to users [5, 23, 1, 8, 22, 17, 3]. Worse, in response to the growing popularity for consumer-protection legislation such as that seen in California in the form of the CCPA and in the EU as GDPR, privacy policies grow longer and more complex each year [23]. One study estimates that if a person were to skim each privacy policy they encountered in one year, it would cost them 81 hours of their time [1].

In response, academics, corporate research groups, and government regulators have come up with myriad observations, strategies, metrics, and design principles to help guide the creation of privacy policies that effectively convey the data use, data collection, and undertaking of risk that users consent to on a daily basis. A recurring and increasingly common observation from these studies is that privacy policies are too long and too complex [1, 3, 28]. To address this, methods of simplifying and condensing privacy policies into user-focused summaries or displays have been proposed. [20, 3].

One such proposal, "Privacy Nutrition Labels", suggests the implementation of a clear and standardized single-page summary of a company's privacy policy, much like how nutritional facts are displayed on food products in many countries. This approach is applied in other contexts as drug facts, energy ratings on appliances, and is the subject of FTC (Federal Trade Commission) commissioned research for the development of a financial privacy notice [1].

In 2020 Apple released a new feature - App Privacy Labels on the iOS, iPadOS, and macOS App Store. The Apple implementation of this feature falls close in line with "Privacy Nutrition Labels" and is a required feature on the App Store page for all apps developed for iOS, iPadOS, and macOS. The release of this feature to roughly 60% of US smartphone users immediately solved a major scalability and adoption problem. It simultaneously provided an opportunity to investigate the open questions left unanswered by Kelley et. al.

We set out to investigate these open questions regarding the use and reception of Privacy Labels in the real world. To our knowledge, this is the first independent study that evaluated the efficacy of a standardized privacy label deployed at scale and to real end users. We collected survey responses from 56 iOS users who were asked about their experience with App Privacy Labels. Specifically, we asked whether they felt the information displayed in the labels influenced their decision to use an app or service, and whether they felt the information displayed in the labels was novel and relevant.

II. Background and Related Work

Over the last decade, there has been increasing public and regulatory demand for more policy, transparency, and overall attention surrounding how companies use the data they collect from users.

A number of high-profile incidents revealed that companies had collected users' private data without consent and, even in cases where the data had been obtained with consent, used it in ways not originally intended nor disclosed [24, 7, 6].

These incidents attracted wide media coverage and sparked public conversation about data collection, data usage, and the privacy practices of large and ever-growing corporations.

At the same time, lawmakers and regulatory bodies began to act. In 2016, the European Parliament and the Council of the European Union passed the General Data Protection Regulation (GDPR) and In 2018, the California State Legislature passed the California Consumer Privacy Act (CCPA). That same year, the chief executives of Facebook (Meta Inc., NYSE:META) and Google (Alphabet Inc., NYSE:GOOG) were asked to testify before Congress about their companies' data collection practices, the former testifying in a hearing titled "Facebook, Social Media Privacy, and the Use and Abuse of Data" [25, 19, 30, 9].

In response to this changing climate surrounding the protection of consumer data, technology companies began attempting to increase transparency and return control over personal data to their users. Google introduced a feature named Privacy Checkup, which lets users decide if and for how long the company can collect their privacy, from search history to geolocation data on photos. [14]

In 2019, Facebook, under intense public and regulatory scrutiny since the Cambridge Analytica incident, introduced a feature named Off-Facebook Activity, which shows users which websites and apps shared the user's data with Facebook and lets the user remove the permissions for those websites and apps [13]. In addition, one unintended consequence of such increased public focus, regulatory pressure, and internal corporate motivation was that actual privacy policies and privacy practice disclosure documents grew long and complex, making them increasingly difficult for end users to understand. Indeed, research showed that users had a poor understanding of data collection and privacy practices [3, 17, 23].

There is a large body of academic, corporate, and regulatory research surrounding privacy policies and myriad observations, heuristics, tools, proposals, and guidelines for how to effectively and concisely convey privacy practice information to end users in the form of privacy policy documents [5, 23, 1, 8, 22, 17, 3, 28].

In particular, our work is motivated by "Privacy Nutrition Labels". The study, conducted by Kelley et. al – was a joint project by researchers at Carnegie Mellon University and Microsoft and laid much of the groundwork for simplified and standardized privacy notices. It indicated that such a label greatly improves the user experience of privacy policies.

Kelley et. al found that many of the 24 participants in the study used the standardized privacy labels to quickly compare different companies and make informed decisions at a glance [1]. While promising, this study was the first in this context, had a limited sample size, and left open a number of unanswered questions, mostly surrounding how end users in the real world would make use of such a label [1, 3]. Practical challenges also stand in the way of meaningful implementation and evaluation and of approaches like Privacy Nutrition labels; low adoption rate and scalability hurdles are frequently mentioned when discussing standardized or simplified privacy policies [3, 16].

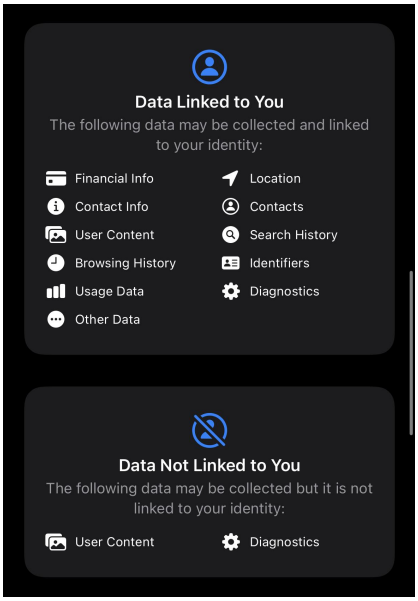
These concerns were seemingly addressed when, in December 2020, Apple released an implementation of Privacy Nutrition Labels called "App Privacy Labels". The labels implement many of the strategies proposed by Kelley et. al. – they are meant to provide users with glanceable, easy to understand information about the type of data that apps collect and how the data is linked to their identity.

App Privacy labels appeared in the app store concurrently with the release of iOS 14.3 on December 14, 2020. Prior to release, App Developers were required to create a privacy label for their app by December 8th, 2020 if they wished for their app to remain on the App Store. It is important to note that all information on the privacy label is self-disclosed by the app developer, and Apple is not explicitly forthcoming about the veracity of the third party disclosure [12]. Indeed, the privacy labels of some apps have been found to be inaccurate; some labels failed to disclose types of data that were actually being collected by the app in question [10]. While extremely important, the trustworthiness of the self-reported disclosures is out of the scope of this paper and should be the topic of further research.

The information on every privacy label on the App Store is divided into three categories: data used to track you, data linked to you and data not linked to you. Examples of "data used to track you" include a user's user ID contact information, which apps can use to identify users even when using another app or browsing an unrelated website [4!]. In addition, when opening the app for the first time, apps that use "data linked to you" to track users' behavior ask for consent to "track your activity across other companies' apps and websites" using contact information and the system advertising identifier (IDFA) [2].

Examples of "data linked to you" include users' purchase history and approximate location. Finally, data that apps collect but are not linked to a users' identity are classified as "data not linked to you". Examples include diagnostics information, which may be used by the developers to improve the user experience [15]. These data categorizations in Apple's App Privacy Labels are closely in line with the categories proposed by Kelley et al.

Figure 1: The App Privacy Label for Google Chrome.



We thus seek to validate the results of Kelley et al on a real world population and further investigate user perception of choice and agency. We gathered survey responses from Apple users (iOS, iPadOS, and macOS) who were asked questions about their experiences with App Privacy Labels on the App store. Our survey questions focused on user perceptions of privacy and aimed to measure the efficacy of the privacy labels compared to traditional long-form privacy policy and privacy notices. We surveyed whether not users learned novel information, and whether the information was important to them personally. Finally, we evaluated whether users believed that the information on privacy labels had a significant impact on their decision to use an app or service, and whether this information had actually caused them to refrain from downloading an app after viewing the privacy label.

III. Approach

We used Google Forms within the NYU organization to create a survey with 14 questions. The questions were either yes-or-no or Likert-Scale, where the respondent is asked to use a scale of 1 to 5 to indicate how much they agreed with the statement presented to them. The questions centered around users' experience with the App Privacy Labels and their general perceptions of digital privacy. At the beginning of the survey, we require participants to read and respond to a consent document that briefly introduces the study and explains how their responses will be used and stored.

We disclosed that participants' email addresses are collected so that their response could be identified should they ask it be removed. The contact information of the Institutional Review Board (IRB) is provided. Before collecting any survey responses, we asked the respondents to indicate whether or not they consented to the statements and information displayed on the consent form, and whether they consented to participation in the research study. If the respondent indicated that they did not agree to any of the terms, the survey immediately ended. No participants indicated that they did not consent to the research.

As a screening measure, we asked whether the respondent has downloaded an app from the iOS, iPadOS or macOS App Store. This question is intended to exclude participants who were not actually Apple product users. Participants who answered in the negative to this question were shown the "survey end" screen and were not asked to participate further. 1 participant indicated that this was the case and was excluded from the remainder of the study. The next three questions were shown to all participants, regardless of their familiarity with App App Privacy Labels.

The first question asked the respondent to indicate to what degree the data collected by companies mattered to them. The respondent was asked to indicate their response on a Likert scale ranging from (1 - "not at all", 5 - "very much so"). The second question asked the respondent to indicate to what degree the type of data that companies collected about them mattered to them on the same Likert scale.

We presented the third question on a separate survey page from the previous two questions to encourage participants to answer this question honestly and without pressure from their responses to the previous two questions. We asked the respondents whether or not they had actually sought out and read privacy policies. We asked participants to indicate their response to this question on a Likert Scale ranging from (1 - "never", 5 - "always"). We then showed the participants a sample privacy label from the App Store page of the mobile browser "Google Chrome" and asked them to indicate whether or not they had seen a similar label before in a yes or no question. The participant's answer to this question determined which of the following four questions they were presented with in the final part of the survey.Both groups of participants were shown the example privacy label for Google Chrome while they responded to the set of questions.

If the participant was familiar with the privacy labels, we asked them to indicate on a Likert Scale (1 - not at all, 5 - very much so) how accurately the following statements represented them.

1. I care about the information presented in labels like this.

2. I am usually already aware of the information shown on these labels.

3. The information labels like the one above influences whether I choose to download an app

4. Information on labels like these has resulted in me choosing not to download an app or in me seeking an alternative.

The questions were centered around whether the participants felt that 1) the labels presented relevant information to the user, 2) the labels presented novel information, 3) the labels empowered the users to make a choice and, finally, whether or not 4) the labels actually influenced the purchase and download decisions of survey respondents. However, we did not question what specific information on a privacy label resulted in the user making the choice not to download the app – we hope that further research will explore this question. If the participant indicated that they used the App Store but were not familiar with the privacy labels, we asked them to indicate on a Likert Scale (1 - not at all, 5 - very much so) how accurately the following statements represented them.

1. The information presented on the label shown above is important to me.

2. I would already be aware of the information shown on labels like the one above.

3. Information shown on a label like this would influence whether I choose to download an app.

4. I am likely to keep an eye out for Privacy Labels in the App Store moving forward.

The questions in this section were centered around whether participants who were not aware of App Privacy Labels would find value in them. We hoped to gauge whether users simply disregarded the privacy labels as unimportant information or whether they cared about the information but were somehow unaware that it was available to them. It must be noted that App Privacy Labels are not visible without scrolling on iOS devices; a user who enters an app's App Store page and immediately clicks download would not see the Privacy Label since it lies further down on the page.

The survey was primarily distributed to students in the NYU Tandon School of engineering. To facilitate the distribution, we asked the Department of Computer Science and Engineering at New York University Tandon School of Engineering (NYU Tandon) for their kind assistance in sending a mass email to all undergraduate and graduate students in the Department. Additionally, we recruited some participants in the study via personal messages/email (for respondents known to the investigators), and group messages sent through NYU Slack channels and Discord servers. Some participants personally known by the investigators were not members of the NYU community, and some NYU participants recruited through NYU Slack channels or Discord servers were not members of the School of Engineerings.All participants were shown the recruitment message described in the IRB. Responses were stored in the NYU Organization's Google Sheets cloud storage and are to be deleted upon the submission of this paper. We did not receive any requests from participants to withdraw from the study.

IV. Ethics

The survey presents minimal risks to the participants and was designed to not include questions that were intrusive, distressing, or contingent on personally identifiable information. Participants consented to have their information used for the purposes of this study. The survey collected email addresses and users were given the option to withdraw from the study at any time before the data was terminated at the end of this study. Overall there were minimal ethical concerns.

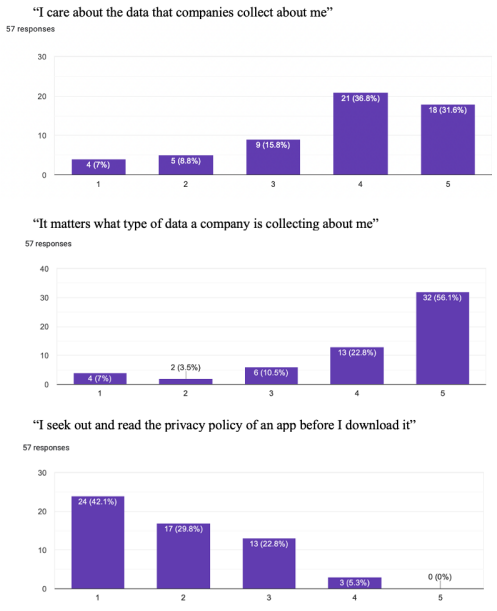
V. Evaluation

A key element of assessing the efficacy of Apple's App Privacy Labels is comparison with the previous or existing model. Before the implementation of the privacy labels, users would only learn about privacy information if they sought out the app's long-form and nonstandard privacy policy on their own or when they received prompts indicating that the app was requesting for access permissions on their device. The majority of respondents indicated that they cared about the information that companies collected about them.

An even more significant majority indicated that it mattered to them what type of data a company was collecting from them. Some respondents indicated that they cared only moderately about the data the companies collected about them but indicated that it mattered to them a great deal what type of data a company was collecting about them.

This suggests that labels that categorize and clearly display the types of information collected by a service would be of value to users and might convince users who would not otherwise care about data collection to pay closer attention to their digital privacy. However, as expected, the third question indicated that the majority of respondents never or almost never read the privacy policy of an app before they downloaded this. This conflict between responses to the first two questions and responses to the third as seen in Figure 2 is consistent with the privacy paradox. In addition, these responses are consistent with prior research suggesting that privacy policies are ineffective at informing users due to their length and complexity [5]. We suspect that any extra steps required to view a privacy policy further disincentivizes users from reading them.. Ultimately it is clear that the existing model of long-form privacy policies are not an effective way to communicate information to the user, in large part due to the fact that users simply never read them.

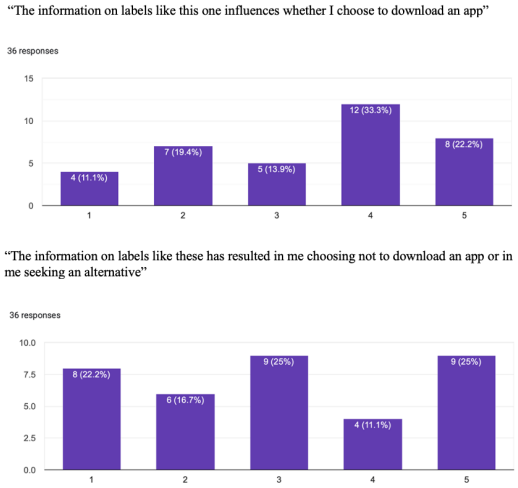
Figure 2: The majority of users are concerned about data collected about them but do not read privacy policies



Efficacy of Privacy Labels

The responses to the questions concerning respondents' experience with App Privacy Labels indicate that privacy labels are more effective at informing users of data collection practices than privacy policies. We found that the majority (63.2%) of users indicated that they were familiar with App Privacy Labels, despite them not being advertised or otherwise promoted on an app's App Store page. The majority (83.3%) of respondents indicated that the information displayed on App Privacy Labels mattered to them. However, the majority of respondents indicated that they were usually already aware of the information presented on App Privacy Labels (61.1%). Only 22.3% of respondents indicated that they were usually unaware of the presented information. We have reason to believe that limitations on the survey population contributed to this result; this is discussed further in the Limitations section. Still, the majority of respondents indicated that the information displayed on the labels influenced their decision on whether or not to download an app (55.5%). Of these, a significant number of respondents indicated that it played a large role in their download decision (22.2%). Whether the information on labels resulted in actual changes in download behavior is less clear. When asked if App Privacy Labels has actually resulted in them not downloading an app or in them seeking an alternative represented them, roughly an equal number of respondents indicated that the statement represented them "not at all", "unsure", and "very much so" (22.2%, 25%, 25%).

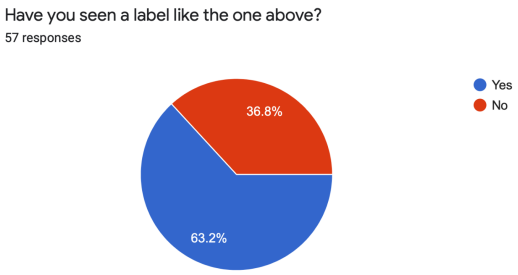
Figure 3: Mismatch between perceived influence on download decision and actual influence on download decision.



This indicates that users are likely to overestimate the degree to which knowledge about a companies' data collection practices ultimately influences their decision to purchase an app. Alternatively, it is possible that the information on App Privacy Labels actually influence their decision a great deal but is overshadowed by much stronger factors such as lack of alternatives, peer pressure, and more. Nonetheless, the results demonstrate that privacy labels effectively provide valuable and previously unknown information to users who would otherwise not seek out such information on their own.

Unfortunately, a significant minority of respondents indicated that they were unaware of the privacy labels altogether.

Figure 4: A significant minority of participants were not familiar with App Privacy Labels.



Amongst this group of respondents, a similar percentage reported that the information on the sample label was important to them (80.9%) as did the same in the group that reported familiarity with the App Privacy Labels (83.3%). A much larger percentage of respondents in this group indicated that they would not be aware of information presented on such a label (52.4%). While the responses to the first question indicate that perceptions of privacy do not seem to influence the likelihood that a respondent was aware of App Privacy Labels, responses to the second question seem to indicate that users who were not aware of App Privacy Labels are less likely to be aware of data collection practices in general. Respondents from this group did not significantly differ in their responses from the other group when asked if the information on the label would influence their download decision.

Finally, we asked users who were unaware of the existence of App Privacy Labels whether they would be likely to keep an eye out for them moving forward.

The majority of users indicated that they were likely to do so (66.4%). There is a strong likelihood of self-bias affecting the responses to this question, especially after respondents presumably just learned about App Privacy Labels. Thus, the responses to this question only inform our general recommendation that App Privacy Labels be promoted by Apple to reach more users.

In total, our study shows that App Privacy Labels are an effective implementation of "Privacy Nutrition Labels" and provides glanceable access to information that the majority of users considers important. The majority of respondents indicated that they were exposed to information that they were not previously aware of and that influenced their decision to download an app.

VI. Limitations

There were a number of limitations in our study design. First, our study involved asking respondents for qualitative estimates of how much they value privacy. We expected some self-reporting bias by users over-reporting how much privacy mattered to them and affected their actions. We considered this in our interpretation of the data. Second, the survey was primarily distributed to NYU students, particularly those of the Tandon School of Engineering. A significant portion of respondents were enrolled in courses related to Computer Science. We hypothesized that this population was more likely to be aware of the information presented on privacy labels and might be less likely to indicate that they learned novel information. We also hypothesized that this population would be more likely to indicate that data collection practices are important to them personally. Due to the nature of our study, we were unable to compare the distribution of our respondents to those from a randomly sampled population.

We acknowledge that these limitations in our survey demographic combined with the relatively low number of respondents (56) may result in a slight overestimate in our observation that users found the information in Privacy Labels to be valuable. Additionally, we acknowledge the potential for an underestimate in our finding that the majority of users who are aware of App Privacy Labels are usually already aware of the information presented in them. Nonetheless, we believe that our results are largely generalizable to a standard technologically literate population.

VII. Conclusion and Future Work

To our knowledge, this is the first study of the efficacy of a standardized "Privacy Label" on a real-world implementation deployed at scale to end users. We find that Apple's App Privacy Labels, their implementation of "Privacy Nutrition Labels" is effective at providing easy access to important information that users consider valuable and actualizes the proposed benefits of simplified privacy policy. We believe that further research is needed to discover what classes and specific categories of data are likely to influence a download decision the most. In addition, the discrepancy between perceived influence on download decisions and actual change in behavior should be further investigated. To validate these results, a broader and larger qualitative survey is needed in order to make a more generalizable claim on the efficacy of privacy labels.

References

[1] Aleecia M. McDonald and Lorrie Faith Cranor ,The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society 2008 Privacy Year in Review issue [pdf]

[2] Apple Support. "If an App Asks to Track Your Activity." *Apple Support*, Apple Support, 27 Apr. 2021, https://support.apple.com/en-us/HT212025.

[3] A. Rao, F. Schaub, N. Sadeh, A. Acquisti, and R. Kang, "Expecting the unexpected: Understanding mismatched privacy expectations online," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, 2016, pp. 77–96.

[4] Chen, Brian X. "What We Learned From Apple's New Privacy Labels." *The New York Times*, The New York Times, 27 Jan. 2021, https://www.nytimes.com/2021/01/27/technology/personaltech/apple-privacy-labels.html.

[5] C. Jensen and C. Potts. Privacy policies as decision-making tools: An evaluation of online privacy notices. In Proc. CHI '04, pages 471–478. ACM, 2004.

[6] Clauser, Grant. "Amazon's Alexa Never Stops Listening to You. Should You Worry?" *The New York Times*, The New York Times, 8 Aug. 2019, https://www.nytimes.com/wirecutter/blog/amazons-alexa-never-stops-listening-to-you/.

[7] Confessore, Nicholas. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far." *The New York Times*, The New York Times, 4 Apr. 2018, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

[8] F. Cate. The Limits of Notice and Choice. IEEE Security & Privacy, 8(2):59–62, Mar. 2010.

[9] Feiner, Lauren. "Apple, Google, Amazon and Facebook CEOs Agree to Testify Before House Committee." *CNBC*, CNBC, 6 July 2020, https://www.cnbc.com/2020/07/01/apple-google-amazon-and-facebook-ceos-to-testify-in-congress.html.

[10] Fowler, Geoffrey A. "I Checked Apple's New Privacy 'Nutrition Labels.' Many Were False." *The Washington Post*, WP Company, 31 Mar. 2021, https://www.washingtonpost.com/technology/2021/01/29/apple-privacy-nutrition-label/.

[11] Hamza Harkous, Kassem Fawaz, Rémi Lebret, Florian Schaub, Kang G. Shin, and Karl Aberer. "Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning". USENIX Security Symposium 2018. (CLASS READING)

[12] Ikeda, Scott. "How Much Will the New Apple 'Privacy Labels' Be Worth If All Data Collection Is Self-Reported?" *CPO Magazine*, CPO Magazine, 7 July 2020, https://www.cpomagazine.com/data-privacy/how-much-will-the-new-apple-privacy-labels-be-worth-if-all-data-collection-is-self-reported/.

[13] Isaac, Mike. "Facebook's New Tool Lets You See Which Apps and Websites Tracked You." *The New York Times*, The New York Times, 20 Aug. 2019, https://www.nytimes.com/2019/08/20/technology/facebook-tool-privacy-apps-websites.html.

[14] Klosowski, Thorin. "10 Practical Privacy Tips for Your Android Phone." *The New York Times*, The New York Times, 28 Apr. 2020, https://www.nytimes.com/wirecutter/guides/privacy-tips-for-android-phone/#give-your-google-account-a-privacy-check-up.

[15] Klosowski, Thorin. "We Checked 250 IPhone Apps--This Is How They're Tracking You." *The New York Times*, The New York Times, 6 May 2021, https://www.nytimes.com/wirecutter/blog/how-iphone-apps-track-you/.

[16] L. F. Cranor. Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. Journal on Telecommunications and High Technology Law, 10:273, 2012.

[17] McDonald, A. M., & Cranor, L. (2010). Americans' attitudes about internet behavioral advertising practices. Paper presented at the Proceedings of the 9th annual ACM workshop on Privacy in the electronic society, Chicago, Illinois, USA.

[18] Newman, Lily Hay. "Apple's App 'Privacy Labels' Are Here—and They're a Big Step Forward | WIRED." *Wired*, WIRED, 14 Dec. 2020, https://www.wired.com/story/apple-app-privacy-labels/

[19] The New York Times. "Mark Zuckerberg Testimony: Senators Question Facebook's Commitment to Privacy." *The New York Times*, The New York Times, 10 Apr. 2018, https://www.nytimes.com/2018/04/10/us/politics/mark-zuckerberg-testimony.html.

[20] P.G.Kelley, J.Bresee, L.F.Cranor, andR.W.Reeder,"A"nutrition label" for privacy," in Proceedings of the 5th Symposium on Usable Privacy and Security, ser. SOUPS '09. New York, NY, USA: ACM, 2009, pp. 4:1–4:12.

[21] PILTON, C., FAILY, S., and HENRIKSEN-BULMER, J. 2021. Evaluating privacy: determining user privacy expectations on the web. Computers and security [online], 105, article 102241. Available from: https://doi.org/10.1016/j.cose.2021.102241

[22] President's Council of Advisors on Science and Technology. Big data and privacy: A technological perspective. Report to the President, Executive Office of the President, May 2014. https://nida.nih.gov/sites/default/files/ispab_jun2014_big-data-privacy_blumenthal.pdf

[23] The Privacy Policy Landscape After the GDPR: Thomas Linden, Rishabh Khandelwal, Hamza Harkous and Kassem Fawaz, Proceedings on Privacy Enhancing Technologies, Volume 2020, Issue 1. (CLASS READING)

[24] Rosenberg, Matthew, et al. "How Trump Consultants Exploited the Facebook Data of Millions." *The New York Times*, The New York Times, 17 Mar. 2018, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[25] S.Hrg. 115-683 — FACEBOOK, SOCIAL MEDIA PRIVACY, AND THE USE AND ABUSE OF DATA. (2022, May 2). https://www.congress.gov/event/115th-congress/senate-event/LC64510/text

[26] Southern, Matt G. “DuckDuckGo Blasts Google Over New IOS Privacy Labels.” *Search Engine Journal*, SearchEngineJournal, 17 Mar. 2021, https://www.searchenginejournal.com/duckduckgo-blasts-google-over-new-ios-privacy-labels/399452

[27] S. Zimmeck, Z. Wang, L. Zou, R. Iyengar, B. Liu, F. Schaub, S. Wilson, N. Sadeh, S. M. Bellovin, and J. Reidenberg, “Automated analysis of privacy requirements for mobile apps,” in *24th Annual Network and Distributed System Security Symposium, NDSS 2017*, 2017. https://usableprivacy.org/files/news/NDSS17.pdf

[28] Tony Vila, Rachel Greenstadt, and David Molnar, “Why We Can't Be Bothered to Read Privacy Policies Models of Privacy Economics as a Lemons Market,” *ACM International Conference Proceeding Series* 50 (2003): 403–407.

[29] V.M. Wottrich, E.A. van Reijmersdal, E.G. Smit “The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns” Decis. Support Syst., 106 (2018), pp. 44-52 https://www.sciencedirect.com/science/article/pii/S0167923617302221

[30] Wakabayashi, Daisuke, and Cecilia Kang. “Google's Pichai Faces Privacy and Bias Questions in Congress.” *The New York Times*, The New York Times, 12 Dec. 2018, https://www.nytimes.com/2018/12/11/technology/google-pichai-house-committee-hearing.html.