Going Beyond Labels

Shakthidhar Reddy Gopavaram[1], Jayati Dev[2], Ece Gumusel[3], and L. Jean Camp[4]

[1]sgopavar@iu.edu
[2]jdev@iu.edu
[3]egumusel@iu.edu
[4]ljcamp@indiana.edu
Indiana University Bloomington

***Abstract*—Currently, consumers have little to no information about the security and privacy offered by an IoT device in the marketplace. This lack of effective communication has hindered consumers' ability to differentiate between secure and insecure IoT devices. Additionally, since consumers can't distinguish between secure and insecure products, companies lack robust incentives to invest in producing secure IoT devices. The result is a market of security lemons. One of the proposed solutions to this problem is to create effective labels. Research has shown that privacy and security labels can help consumers distinguish between secure and insecure IoT devices; yet labels alone do not guarantee that consumers will choose secure devices over insecure ones. One reason for this is that, beyond information asymmetry, consumers' decision-making is also affected by lack of technical knowledge, bounded rationality, and psychological biases. Consumers may not want to pay a premium for better security if they do not believe the claims made about the premium product. In this paper, we build on past work in economics of security to outline a set of recommendations for labeling. We also provide recommendations for how the design of the marketplace can address factors in human decision-making to best align consumer decisions with their preferences over the long term.**

I. Introduction

Consumers state that their privacy and security are important to them but often make decisions that are not in line with these preferences. One reason for this paradox is information asymmetry. Consumers don't have access to information about the privacy and security offered by a device. However, that is not the only cause for the discrepancy between preferences and behavior. Even when users have privacy and security risk information in the form of labels, they can still make decisions that are not in line with their preferences. This is because decision-making is also affected by bounded rationality and psychological biases. So it is necessary to take these factors into account when designing privacy and security labels.

The paper is organized as follows: In section 1, we build upon past work in risk communication to provide a set of recommendations for designing labels. We discuss the different types of labels (Binary, Graded, and Descriptive), bounded rationality (refers to cognitive limits of users that bound their ability to process information presented to them), framing, and choice of icons. In section 2, we talk about the psychological biases that influence consumers' decision-making processes. Specifically, we will be discussing the impact on endowment effect and status-quo bias on users' decision making. Finally, Section 3 concludes with a discussion on future work.

S. Gopavaram, J. Dev, E. Gumusel, L.J. Camp. **Going Beyond Labels**. *Response to NIST Calls for Submission to the Workshop on In Workshop and Call for Papers on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT)*, September 2021. https://www.nist.gov/system/files/documents/2021/09/03/IndianaUniversity-NIST_Beyond_Privacy_Labels.pdf

II. Information Asymmetry and Privacy Labels

Information asymmetry occurs when a seller has information about the type or quality of a good that is unknown to the buyer [3]. In our case, consumers who don't have information about the privacy and security are offered by an IoT device. So they are unable to distinguish between secure and insecure devices. The obvious solution to this problem is to present users with relevant information. However, the manner of presentation matters, and it determines if users can make informed decisions. For example, information about the data collection and usage practices associated with IoT devices are communicated through privacy notices and policies. Although these privacy policies are notoriously unusable [28], [13]. There are a few reasons for this:

1) Privacy policies often span multiple pages and require a significant investment of time from the user [22], [20].
2) Privacy policies contain complex legal terminology and are beyond the comprehension of people who have less than or equal to a high school education [14].
3) Given the time investment and the incomprehensibility of these privacy policies, it would be virtually infeasible for a person to compare multiple policies.

Past research has proposed three types of labels. These are Binary Labels, Graded Labels, and Descriptive Labels [8], [5].

A. Binary Labels

Binary labels are essentially a privacy/security seal. The existence of a privacy/security seal indicates that a product is privacy-preserving and secure. The absence of the same seal implies the opposite. These are similar to the seals you find in the food and agriculture industries (e.g., USDA's organic seal). In the past, binary labels like TRUSTe, BBCOnline, and CPAWebTrust were used to communicate trust in the web domain [21]. The intention was to help consumers identify websites that employ practices consistent with regulatory expectations and standards for privacy accountability. While

these labels address the three points mentioned above, past research has found them to be ineffective [21], [12]. The primary reason for their failure is the lack of familiarity with the labels and what they represent [21], [12]. Therefore, consumer education campaigns designed to familiarize people with the graphical representation of the seal and its function are necessary for the success of binary seals.

Even when familiarity with the seal and its function is not an issue, binary labels may be less effective when compared to graded and descriptive labels [16].

B. Graded Labels

Graded labels or privacy and security ratings have been used in past works to inform people about the privacy and security risks associated with web applications, mobile apps, and IoT devices [27], [23], [10], [9]. In particular, Rajivan et al. conducted a study to inform the choice of icons and framing for communicating aggregate risk. In that study, the authors compared stars, locks, and eyes (based on [25]) using both positive and negative framings. They found the use of positively framed aggregate risk ratings using the lock icon to be most effective [23].

Johnson et al. evaluated the effectiveness of graded labels for communicating IoT security risk [16]. They found that consumers were more likely to select devices with the highest security rating when compared to devices with mid to low-level security ratings [16]. They also reported that 48% of the participants requested information about what the different grades meant, how the security grades were calculated, and what risks a device with a certain rating reduced [16].

C. Descriptive Labels

Descriptive labels do not provide consumers any information about the level of privacy/security offered by a device or application. They simply list the practices that impact privacy and security. One prominent example of descriptive labels is the permissions manifest utilized in the Android PlayStore. The manifest was provided to the user at the time of app installation and listed all the sensitive resources the app would be able to access. Consumers had to self-evaluate the risk and take appropriate action (install or not install the app). Past research has shown that permissions manifests are ineffective at communicating risk to the user [4], [6], [7], [23], [10].

Descriptive labels for Android applications were ineffective because the everyday consumer does not have the technical knowledge to understand the permission presented to them and their implications [7], [17].

III. Endowment Effect and Status-Quo Bias

People often attribute a higher weight to the items they possess when compared to the items they don't [18], [2], [11], [1], [9]. This discrepancy between Willingness-To-Pay(WTP) and Willingness-To-Accept(WTA) is known as the endowment effect. Past research has shown that people attribute a higher value to privacy/security in the WTA condition when compared to the WTP condition [2], [11].

Staus-quo bias is a preference for the current state of affairs [24], [26]. Status-quo bias can be explained by two components: (1) loss aversion and (2) omission bias. People are inherently loss-averse, so they tend to attribute a higher value to their losses associated with a change in state when compared to the gains [24], [26]. Furthermore, people react more adversely to negative outcomes caused by taking an action as opposed to the same outcomes when they result from inaction [24]. Therefore, a combination of the two factors prevents people from taking any action to change the default.

Status-quo bias has been observed in situations where websites or other services ask users for their consent to collect personal information. For example, when the check box for consent is checked by default, most people stick to the default and do not take any action [15], [19].

In the case of IoT, Gopavaram et al. utilized the theories of the endowment effect and status-quo bias to build two versions of an IoT marketplace emulating WTP and WTA scenarios for privacy [9]. The results from that study showed that more people in the WTA condition were willing to pay a premium to purchase devices with the highest privacy rating [9]. At the same time, people in the WTP group were less willing to pay for better privacy despite having the same indicators for privacy risk [9].

Psychological biases, like the endowment effect and status-quo bias, can be used to nudge people towards choosing better security. Especially in scenarios where having better security has minimal benefit for the individual but is of significant benefit to the ecosystem. Additionally, one must make sure that the design of the marketplace does not nullify the positive effects of privacy/security labels.Endowment Effect and Status-Quo Bias.

IV. Recommendations

Based on the past work in risk communication and psychological biases discussed in the previous two sections, we make the following recommendations:

1) Deciphering the information privacy/security labels should not be time-consuming. The labels must be intuitive and easily comprehensible.
2) Consumers should not be required to have the technical expertise to understand the privacy/security labels.
3) Multi-layered privacy/security labels can satisfy both expert and non-expert users by providing simple aggregate labels in the first layer and more detailed information about privacy and security practices in the second layer.
4) Consumer education campaigns are needed to help consumers understand the function of the privacy/security label. They can also help with the success of the label.
5) The design of the marketplace must be evaluated to ensure that they don't counteract the positive effects of the privacy/security labels.
6) Psychological biases can be used to nudge consumers to choose devices with high security and privacy for the betterment of the ecosystem.

We propose a more comprehensive approach to consumer awareness that tackles information asymmetry, bounded ra-

tionality, and psychological biases. Specifically, we recommend the use of multi-layered labels to communicate risk to consumer. Here the first later would present aggregate privacy and security risk information using graded labels. The second layer would contain more detailed information about the privacy and security practices. This two tiered approach would address information asymmetry and bounded rationality by both providing the needed information and enabling easy comparisons between products. The two tiered approach would also address expert consumers' need for more information.

In addition to communicating risk in the marketplace using a multi-layered label, we would also propose modifying the design and presentation of products to nudge consumers towards choosing privacy-preserving and secure products. We believe that this is essential because consumers may not always have the incentive to pay a premium to purchase products with high security as the arising risks may not affect them.

DISCLAIMER

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of any employer, affiliate, or source of research support. These opinions, findings, and conclusions or recommendations do not necessarily reflect the views of the US Government, the National Science Foundation, the National Security Agency, Cisco, Comcast, Google, nor Indiana University.

REFERENCES

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015.

[2] Alessandro Acquisti, Leslie K. John, and George Loewenstein. What Is Privacy Worth? *The Journal of Legal Studies*, 42(2):249–274, 2013.

[3] George A Akerlof. The market for "lemons": Quality uncertainty and the market mechanism. In Peter Diamond and Michael Rothschild, editors, *Uncertainty in Economics*, pages 235 – 251. Academic Press, 1978.

[4] K. Benton, L. J. Camp, and V. Garg. Studying the effectiveness of android application permissions requests. In *2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pages 291–296, March 2013.

[5] John M Blythe and Shane D Johnson. Rapid evidence assessment on labelling schemes and implications for consumer iot security. *Technical Report, DCMS London*, 2018.

[6] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. Android permissions demystified. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 627–638. ACM, 2011.

[7] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android Permissions: User Attention, Comprehension, and Behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 3:1–3:14, New York, NY, USA, 2012. ACM.

[8] Vaibhav Garg. A lemon by any other label. In *ICISSP*, pages 558–565, 2021.

[9] Shakthidhar Gopavaram, Jayati Dev, Sanchari Das, and L Jean Camp. IoT Marketplace: Willingness-To-Pay vs. Willingness-To-Accept. In *Proceedings of the 20th Annual Workshop on the Economics of Information Security (WEIS 2021)*, 2021.

[10] Shakthidhar Reddy Gopavaram, Omkar Bhide, and L. Jean Camp. Can You Hear Me Now? Audio and Visual Interactions That Change App Choices. *Frontiers in Psychology*, 11:2227, 2020.

[11] Jens Grossklags and Alessandro Acquisti. When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information. In *6th Annual Workshop on the Economics of Information Security, WEIS 2007, The Heinz School and CyLab at Carnegie Mellon University, Pittsburgh, PA, USA, June 7-8, 2007*, 2007.

[12] Milena M Head and Khaled Hassanein. Trust in e-commerce: Evaluating the impact of third-party seals. *Quarterly journal of electronic commerce*, 3:307–326, 2002.

[13] Privacy Leadership Initiative et al. Privacy notices research final results. *Conducted by Harris Interactive, December*, 2001.

[14] Carlos Jensen and Colin Potts. Privacy Policies As Decision-making Tools: An Evaluation of Online Privacy Notices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '04, pages 471–478, New York, NY, USA, 2004. ACM.

[15] Eric J. Johnson, Steven Bellman, and Gerald L. Lohse. Defaults, Framing and Privacy: Why Opting In-Opting Out. *Marketing Letters*, 13(1):5–15, Feb 2002.

[16] Shane D Johnson, John M Blythe, Matthew Manning, and Gabriel TW Wong. The impact of IoT security labelling on consumer product choice and willingness to pay. *PloS one*, 15(1):e0227800, 2020.

[17] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. A conundrum of permissions: installing applications on an Android smartphone. In *International Conference on Financial Cryptography and Data Security*, pages 68–79. Springer, 2012.

[18] Jack L. Knetsch. The Endowment Effect and Evidence of Nonreversible Indifference Curves. *The American Economic Review*, 79(5):1277–1284, 1989.

[19] Yee-Lin Lai and Kai-Lung Hui. Internet Opt-in and Opt-out: Investigating the Roles of Frames, Defaults and Privacy Concerns. In *Proceedings of the 2006 ACM SIGMIS CPR Conference on Computer Personnel Research: Forty Four Years of Computer Personnel Research: Achievements, Challenges &Amp; the Future*, SIGMIS CPR '06, pages 253–263, New York, NY, USA, 2006. ACM.

[20] Aleecia M McDonald and Lorrie Faith Cranor. The cost of reading privacy policies. *Isjlp*, 4:543, 2008.

[21] Trevor Moores. Do consumers understand the role of privacy seals in e-commerce? *Commun. ACM*, 48(3):86–91, March 2005.

[22] Victoria C Plaut and Robert P Bartlett III. Blind consent? A social psychological investigation of non-readership of click-through agreements. *Law and human behavior*, 36(4):293–311, 2012.

[23] Prashanth Rajivan and Jean Camp. Influence of Privacy Attitude and Privacy Cue Framing on Android App Choices. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, Denver, CO, 2016. USENIX Association.

[24] Ilana Ritov and Jonathan Baron. Status-quo and omission biases. *Journal of Risk and Uncertainty*, 5(1):49–61, Feb 1992.

[25] Roman Schlegel, Apu Kapadia, and Adam J. Lee. Eyeing Your Exposure: Quantifying and Controlling Information Sharing for Improved Privacy. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, pages 14:1–14:14, New York, NY, USA, 2011. ACM.

[26] Richard Thaler. Toward a positive theory of consumer choice. *Journal of Economic Behavior & Organization*, 1(1):39 – 60, 1980.

[27] Janice Y. Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, 22(2):254–268, 2011.

[28] Joseph Turow, Lauren Feldman, and Kimberly Meltzer. Open to Exploitation: America's Shoppers Online and Offline. *A Report from the Annenberg Public Policy Center of the University of Pennsylvania*, page 35, 2005.