

Types of Privacy Expectations and Mismatches

Ashwini Rao, [ashwini@cs.umich.edu](#), Researcher, Unaffiliated
Florian Schaub, [florian.schaub@umich.edu](#), Assistant Professor, University of Michigan
Under review in IEEE Internet Computing Special Issue on Usable Privacy & Security, May/June 2017

With companies collecting unprecedented amount of personal data, it is becoming increasingly important to understand whether or not such data collection practices match users' data privacy expectations. In this context, we consider the concept of *privacy expectation* as a construct with multiple types or levels. We examine a related concept: *privacy expectation mismatch*. We describe different types of privacy expectations and different types of mismatches. We argue that by treating privacy expectation as a multi-level construct, we can better understand causal links between privacy expectation and constructs such as privacy concern and privacy behavior, and realize how privacy mismatches impact user privacy. We discuss the challenges, recent advances and open questions in this area.

In an increasingly technological world, user interactions with online, mobile and Internet-of-Things technologies is becoming an inherent and unavoidable part of everyday life. The rapid increase in the number and frequency of interactions has made possible an unprecedented amount of data collection and sharing by private and government entities. At the forefront of issues surrounding data practices is whether such practices match user data privacy expectations.

Data practices may or may not match users' privacy expectations. For instance, in a recent study we conducted¹, we found that 90% of participants did not expect banking websites to collect and share health information. However, one of the banking websites in our study did do so thereby violating users' data privacy expectations. The bank has an affiliate that is an insurance provider, and the bank can collect

health information about its users from its affiliate. Although users may have expected the collection of health information in the insurance context, they did not expect it to be collected in the banking context.

Studying data privacy expectations is important for several reasons. Expectations influence decision making,² for example, users' expectations may influence their decision to use or not use a product. Meeting expectations is also linked to consumer satisfaction³. Hence, businesses that want to increase product usage or consumer satisfaction could benefit by understanding users' privacy expectations. By identifying data practices that violate dominant privacy expectations, regulators can create policies that protect consumers from privacy invasive data practices. Studying data privacy expectations can also help in developing new privacy enhancing technologies. For instance,

website privacy policies, which serve as the primary mechanism for notifying users about data practices, in their current format can be long and time consuming to read. Approaches that aim to improve comprehension of privacy policies may benefit by identifying data practices that do not match user privacy expectations. The number of mismatched data practices may be smaller than the total number of data practices, and, hence, highlighting mismatched data practices may reduce the amount of information users have to process.⁴

In our work on studying data privacy expectations, we address three research questions. First, how do we define the concept of privacy expectation? We focus on a specific aspect: privacy expectation types. Our work is inspired by research on customer expectations in customer satisfaction and dissatisfaction (CS/D) and service quality literature. Although, the concept of expectation is not new to the privacy domain, a rigorous investigation of privacy expectation as a construct that can have multiple types or levels is lacking. Our second research question addresses the challenges of measuring privacy expectation types. Our third research question deals with understanding whether data practices align with users' privacy expectations. In this context, we investigate the concept of privacy expectation mismatch, identify different types of mismatches, and analyze the impact of privacy expectation types on mismatches. In the rest of the article, we discuss privacy expectation types, mismatches and challenges in measuring privacy expectation types.

Privacy expectation types

The theoretical background for our work on privacy expectation types comes from the research on customer expectations in customer satisfaction and dissatisfaction (CS/D) and service quality literature. Starting in early 1970, CS/D researchers have conceptualized and provided empirical evidence for existence of multiple customer expectation types that can influence customer satisfaction.^{3,5,6} Based on the work in CS/D domain, in early 1990, researchers in service quality domain investigated and found evidence for different types of customer expectations of service.⁷ We briefly discuss the work on customer expectation types. We then examine existing work on expectations in the privacy domain and highlight the need and importance of investigating privacy expectation types.

Customer expectations

In the CS/D and service quality domains, customer expectations are considered "pre-trial beliefs about a product that serve as standards or reference points against which performance is judged."⁷ The gap between customer expectations and actual performance determines customer assessment of quality or satisfaction. In these domains there is general agreement on the existence of multiple expectation types and also on the causal impact of expectation types on quality and satisfaction.

In the CS/D and service quality domains, there is a lack of agreement on the nature and number of expectation types. For example, in the CS/D domain, Miller conceptualized four expectation types: Ideal, Expected, Minimum Tolerable, and Deserved.³ The Ideal represents what users

think performance can be. The Expected is objective, without an affective dimension, and represents what users think performance will be. The Deserved has an affective dimension and represents what users feel performance should be. Lastly, the Minimum Tolerable is what users think the lowest performance must be. Gilly et al. found empirical support for only three of Miller's expectation types.⁵ Swan and Trawick found two types of expectations: Predictive and Desired.⁶ The Predictive is what users objectively think will happen, and the Desired is what they subjectively want to happen.

Privacy expectations as desires

In the privacy domain, work exists on measuring user privacy preferences. Preferences could be considered as desires or wants of users, for example, what users feel data practices of websites should be. Hence studying preferences can be considered as studying the Deserved ("should") expectation type. Among the privacy research that has explicitly studied privacy expectations, we looked at the wording employed while eliciting expectations. Based on that, we find that some researchers studied desires (e.g. "should allow"). In other studies, on privacy expectations, it is not clear what type of expectation is the focus of inquiry because the wording is ambiguous (e.g. "do you expect"); the word expect can imply what users feel should happen, what they think would happen etc.

Considering the existing work on privacy preferences and expectations, privacy domain has predominantly studied desires or the

Deserved type. Until early 1990, researchers in service quality domain considered customer expectations as predominantly desires or wants of customers i.e. expectations-as-desires standard. In the early 1990, researchers pointed out the need to study other expectation standards, and laid out a framework for doing so.⁷ In our work on privacy expectations, we are following a similar approach.

Privacy expectations as likelihood

We can consider privacy expectations as likelihood or probability, that is, what users think data practices would be and not what they feel data practices should be. In our recent study on identifying mismatches between user expectations and actual website data practices,¹ we elicited user expectations in the likelihood sense. Since, privacy studies show that user privacy behavior differs from user stated preferences, we argued that preferences are not reliable for identifying mismatches between privacy expectations and a company's actual data practices. Borrowing from Miller's conceptual model of expectation types, we explicitly differentiated between privacy expectation in the sense of likelihood of occurrence (Expected type or "will be") and desires or preferences (Deserved type or "should be").

Privacy expectations: other types

Privacy expectations other than desires or likelihood may exist. Users may have privacy expectations that must absolutely hold, e.g., a website must not share health information with advertisers under any circumstance. Users may also have ideal expectations, e.g., in an ideal world, websites could offer not to share email

addressed under any circumstance. Following Miller's terminology, we could label the former as Minimum Tolerable type and the latter as Ideal type.

There could be advantages in studying additional expectation types. For instance, privacy studies such as those related to online tracking show a large gap between user preferences and company data privacy practices. Studies find that most users do not want their personal information collected by advertisers, but advertisers do so regularly and comprehensively to target ads. By eliciting preferences, these studies are measuring desires. However, by considering more expectation types, we could distinguish further between the type of desire e.g. ideal vs. minimally acceptable. When we measure ideal desires, we may find that the gap is larger than when we measure minimally acceptable desires. This has important consequences for addressing consumer privacy needs. From a public policy perspective, privacy regulators could focus on larger gaps. By addressing larger gaps and not smaller gaps, companies could have flexibility in achieving a balance between utility and privacy. For example, while providing tracking services, companies could stop data practices that lead to larger gaps, but retain data practices with smaller gaps.

Privacy expectations: single vs. multiple types

Although privacy research has explored the concept of expectations of privacy, the potential for multiple levels or types of privacy expectations has not received much attention. Seminal work on privacy expectations, has

viewed privacy expectation as a construct with a single level. Nissenbaum proposes contextual integrity as a conceptual framework to understand how expectations of privacy are shaped by context.⁸ In Nissenbaum's work, expectation has a single level whose value may change as context changes. Altman's privacy regulation theory centers on the idea that individuals continuously modify their behavior to achieve a desired level of privacy – they calibrate their expectations between desired and actual levels of privacy when the actual level changes due to other factors.⁹ Although, Altman differentiates between desired and achieved levels, it is not same as differentiating between multiple levels or types of privacy expectations that may exist in users' minds. Moreover, it is important to note that people could have multiple levels of privacy expectations even when all other factors are constant.

In the privacy domain, it is not yet clear what types of expectations should be distinguished. Further research, both qualitative and quantitative, is necessary to comprehensively identify the different privacy expectation types.

The gap between customer expectation type and actual performance can impact assessment of satisfaction and quality. Similarly, the gap between privacy expectation type and actual data practice may impact constructs such as privacy concern, surprise and behavior as well as satisfaction and quality. For example, gap between minimally acceptable desire and reality may better predict privacy concern than gap between ideal desires and reality. However, gap between ideal desires and reality may better predict satisfaction than gap between

minimally acceptable desire and reality. Hence, there is a need to study such causal links.

Distinguishing between privacy expectation types may allow us to understand privacy profiles better. Privacy profiles group users with similar attitudes, beliefs, concerns etc. into a single category. Using privacy profiles, one could make recommendations regarding privacy settings. Research on privacy profiles shows that a large percentage of users fall into the “fence-sitters” or “undecided” category. By using privacy expectation type as an additional predictor variable, it may be possible to distinguish further between users in that category, which may allow better recommendations.

Measuring privacy expectations

Privacy research shows that privacy expectations could vary based on context (e.g. health vs. financial website), user demographic (e.g. younger vs. older users), prior experience etc. Privacy expectations may evolve over time, and measurements may have to be run longitudinally. To measure privacy expectation types, these factors have to be considered.

Another challenge in measuring privacy expectation types via user studies or interactions with consumers is the wording used for conveying the expectation types. In our study¹ on eliciting privacy expectations in the likelihood sense, we framed the questions as likelihood questions. For example, one of the questions was “*What is the likelihood that [website name] **would collect** your information in this scenario?*” In contrast, to measure privacy expectations in the desired sense, we

could frame the question as “*Do you think that [website name] **should or should not be allowed** to collect your information in this scenario?*” Survey research shows that small changes in wording can have a large impact on measurements. With improper wording, the questions may measure the wrong expectation type. With ambiguous wording, a question may convey different expectation types to different users. For example, the question “*Do you **expect** [website name] to collect your information in this scenario?*” may convey either desire (“should collect”) or likelihood (“would collect”).

Mismatched privacy expectations

By comparing privacy expectations, elicited from users, with actual data practices, we can identify whether data practices align with users’ expectations. Understanding matches and mismatches is important for improving public policy and developing privacy enhancing technologies. For example, to shorten a privacy notice, we need not highlight data practices that match privacy expectations, but highlight data practices that do not match.

Consider the scenario where we elicit users’ expectations for a given website data practice e.g. collection of health data. For a given website, we can annotate the data practice as Yes or No. For example, a Yes indicates that the website collects health data, and a No indicates that the website does not collect health data. If users expect the website to engage in the data practice, we can annotate it as Yes. If users do not expect the website to engage in the data practice, we can annotate it as No. When we compare values for the data practice with

values for expectations, we get four combinations: Yes-Yes, Yes-No, No-Yes and No-No. The Yes-Yes and No-No cases indicate a match, and the Yes-No and No-Yes cases indicate a mismatch. In Table 1, we show the two matches and the two mismatches.

Website data practice	User expectation	Match / Mismatch
Yes	Yes	Match
Yes	No	Mismatch
No	Yes	Mismatch
No	No	Match

Table 1. Mismatches in privacy expectations

Implications for privacy: Yes-No vs. No-Yes mismatch

The impact of mismatches on privacy can vary based on the type of mismatch. Below we examine how Yes-No and No-Yes mismatches may impact users' privacy. As we will see, a Yes-No mismatch can impact user privacy, but a No-Yes mismatch cannot. This is true even in the absence of multiple privacy expectation types.

Consider the Yes-No mismatch where a website collects and shares users' information, but users do not expect it to do so. Due to lack of awareness of the website's data practices, users may decide to use the website. By using the website, users give the website access to data that they do not want to be collected or shared resulting in a violation of their data privacy. Now consider the No-Yes mismatch where a website does not collect or share users' data, but users expect the website to do so. As a result, users may decide not to use the website, which may affect their utility but not their data privacy.

Mismatches: impact of expectation types

The type of privacy expectation can change the impact of Yes-No and No-Yes mismatches. By taking into account the type of expectation for a mismatch, we can better understand why a mismatch exists between users' expectation and actual data practice. We can also get more clarity about the implications of a mismatch on user data privacy. Below, we consider Miller's conceptual model of expectation types (Ideal, Expected, Minimum Tolerable, and Deserved), and analyze how they may impact the Yes-No mismatch. We can carry out a similar analysis for the No-Yes mismatch.

Since the Expected ("will") type is objective and devoid of an affective dimension, a Yes-No mismatch for this type stems from users' thinking. The mismatch indicates that the user's knowledge of privacy practices is lacking. Hence, as a remedial measure to address the mismatch, a public policy initiative could educate users how to identify data practices such as collection of health information on banking websites and online tracking.

The Deserved ("should") type has an affective dimension, and, hence, a Yes-No mismatch for this type indicates the role of users' feelings. For example, users with a privacy fundamentalist profile strongly feel that websites should not collect their personal information. Users may or may not be aware whether websites actually collect personal information.

A Minimum Tolerable ("must") type indicates a minimally acceptable scenario (worst case). For example, websites must not share health

information with advertisers. An Ideal (“can”) type indicates an ideal scenario (best case). For example, it would be nice if websites did not share email addresses with advertisers. Hence, a Yes-No mismatch for Minimum Tolerable type can be much more privacy invasive than a Yes-No mismatch for Ideal type. For a remedial measure such a privacy notice that highlights Yes-No mismatches, it is more important to highlight a Yes-No mismatch for the Minimum Tolerable type than the Ideal type. In an effort to shorten such a privacy notice, it may display only Yes-No mismatches for the Minimum Tolerable type.

Website data practice	User expectation		Match / Mismatch
	Expected type ("will")	Deserved type ("should")	
Yes	Yes	Yes	Match
Yes	Yes	No	Mismatch
Yes	No	Yes	Mismatch
Yes	No	No	Mismatch

Table 2. Mismatches resulting from interplay of privacy expectation types

Mismatches: impact of interplay of expectation types

While analyzing mismatches, considering the interplay of expectation types can add an additional dimension to the assessment of matched and mismatched expectations. Below we analyze the interplay of Expected (“will”) and Deserved (“should”) types. Table 2 shows the combinations resulting from the interplay of the two expectation types. We can similarly analyze the interplay of other combinations.

Consider a scenario where we elicit both Expected (“will”) and Deserved (“should”) expectations from users. When the website’s

data practice matches the Expected type elicited from users, we see a Yes-Yes match. However, if we also include the Deserved type into our analysis (Yes-Yes-Yes or Yes-Yes-No), we see a different picture. A Yes-Yes-Yes is a match whereas Yes-Yes-No is a mismatch. Yes-Yes-Yes indicates that website’s data practice matches users’ thinking which in turn matches users’ feeling; users are aware of the data practice and prefer it. Yes-Yes-No indicates a mismatch where users are aware of the data practice but do not prefer it. Unless users are aware of websites that do not have such data practices, they may continue using the website. For example, although users may know that Google's search website collects certain information about them, they may continue to use Google because they are not aware of privacy-friendly alternatives such as DuckDuckGo. Sometimes all websites in a category may have equally privacy invasive data practices, and users may not have a choice. By understanding whether it is lack of awareness or lack of choice, remedial measures such as public policy initiatives can take adequate action.

When the website’s data practice does not match the Expected type elicited from users, we see a Yes-No mismatch. By including the Deserved type into our analysis (Yes-No-Yes or Yes-No-No), we can infer more information about the mismatch. In a Yes-No-No mismatch, the websites data practice does not match both users thinking and feeling; users incorrectly think that a website will not engage in a data practice and also feel that it should not. However, since users’ thinking and preference match, they may use the website and lose their

data privacy. In a Yes-No-Yes mismatch, website's data practice does not match users thinking, but matches users' preference; users think that the website will not engage in the data practice, but prefer that the website do it. For instance, users may want a website to provide personalized services based on their data, and prefer that the website collect their data for that purpose. Since user's thinking does not match their preference, users may not use the website and lose utility, but not data privacy.

Conclusion

Our analysis suggests a nuanced and structured perspective on privacy expectations facilitates a deeper understanding of privacy issues and decision making processes. Treating privacy expectation as a multi-level construct can improve our understanding of other privacy related constructs such as privacy concern. Distinguishing between privacy expectation types e.g. desires and likelihood may explain apparent discrepancies or contradictions in observed user behavior and stated preferences.

Our analysis also shows that different types of mismatches can have important implications for both users and companies and underlines the value of distinguishing among different types of privacy expectations. Examining multiple expectation types allows us to identify the root cause of mismatches.

Knowledge of privacy expectations and mismatches can inform the design of privacy notice and control mechanisms. For instance, mismatches may indicate unexpected practices, which privacy notices can highlight. Furthermore, a better understanding of

expectations and expectation mismatches can provide insights on the effectiveness of existing legal and regulatory requirements surrounding privacy and indicate need for changes in public policy or privacy regulations.

Our goal is to foster a conversation around how we approach privacy expectations research. Although the application of Miller's customer expectation types to privacy expectation types seems intuitive, further research is necessary to validate these types and potentially identify other/additional types of privacy expectations.

Acknowledgement

This research was partially funded by the National Science Foundation under grants CNS-1330596 and CNS-1012763. We are grateful to Alessandro Acquisti, Norman Sadeh and Ruogu Kang for their help with our work on privacy expectations. We thank Birendra Jha for help with the manuscript.

References

1. A. Rao et al., "Expecting the Unexpected: Understanding Mismatched Privacy Expectations Online." *Proc. 2016 Symp. on Usable Privacy and Security*, 2016, pp. 77-96.
2. R. M. Hogarth, "Judgement and Choice: The Psychology of Decision." John Wiley & Sons, 1987.
3. J. A. Miller, "Studying satisfaction, modifying models, eliciting expectations, posing problems, and making meaningful measurements." *Proc. 1977 Conceptualization and Measurement of Consumer Satisfaction and Dissatisfaction*, 1977, pp. 72-91.
4. J. Gluck et al., "How Short Is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices." *Proc. 2016 Symp. on Usable Privacy and Security*, 2016, pp. 321-340.
5. M. C. Gilly et al., "The expectations-performance comparison process: An investigation of expectation types." *Proc. 1983 Conf. on Consumer Satisfaction, Dissatisfaction, and Complaining Behavior*, 1983, pp. 10-16.

6. J. E. Swan and F. I. Trawick, "Satisfaction related to predictive vs. desired expectations." *Proc. 1980 Refining Concepts and Measures of Consumer Satisfaction and Complaining Behavior*, 1980, pp. 7–12.
7. Zeithaml et al., "The nature and determinants of customer expectations of service." *Proc. 1993 Academy of Marketing Science*, 1993, vol. 21(1), pp. 1–12.
8. H. Nissenbaum, "Privacy in Context - Technology, Policy, and the Integrity of Social Life." Stanford University Press, 2009.
9. I. Altman, "The environment and social behavior: Privacy, personal space, territory, and crowding." Brooks/Cole, 1975.