Factors Affecting Perceptions of Privacy Breach among Smartphone Application Users

Stanislav Mamonov
The Graduate Center, CUNY
Zicklin School of Business
Stanislav.Mamonov@baruch.cuny.edu

Raquel Benbunan-Fich
Zicklin School of Business
Baruch College
Raquel.Benbunan-Fich@baruch.cuny.edu

Abstract
Drawing on psychological contract theory, we experimentally examine four factors affecting perceptions of privacy breach among smartphone application users. We investigate the effects of the type of information which is perceived to be misappropriated by the application, the presence of legal agreement giving application developers rights to use the information, the source of information suggesting that a privacy breach may have occurred and the application type (free or paid). We find that perceptions of misappropriation of financial information are more distressing than perceived misappropriation of geo-location data. The presence of legal contracts giving application developers rights to information only partially attenuates perceptions of privacy breach among application users. This study offers a novel theoretical perspective and a new focal construct of perceived privacy breach for future research on privacy. Additionally, this study highlights the practical limitations of legal contracts in preventing perceptions of privacy breach.

1. Introduction
Privacy is an important topic for both theory and practice. Technology continues to permeate daily activities and makes it easier to gather personal information about technology users. The importance of privacy is highlighted by the fast adoption of smartphones. Recent estimates indicate that smartphone shipments have surpassed deliveries of personal computers and industry projections suggest that nearly a billion smartphones will be sold worldwide in 2013 [17]. The growing adoption of smartphone technology is driven by a wealth of functionality provided by third party applications. For example, over 1 million applications have been approved for Apple’s app store [12]. These apps enable users to carry out a variety of activities including banking and shopping. As a result, it is not surprising that mobile commerce represents a large and increasing market opportunity and that it already contributes $8 billion to the US economy [11]. While smartphones offer many benefits, they also expose smartphone users to growing privacy risks. A recent survey revealed that 70% of smartphone users express concerns about their privacy [38]. These findings suggest that the industry continues to struggle with privacy-related issues and the topic merits further research.

While there is a substantial body of research on privacy [22], much of prior research in Information Systems has focused on privacy-related concerns [33], as opposed to the way in which privacy breaches are perceived. Privacy concerns play an important role at the initiation of relationships which expose participants to privacy risks. Notwithstanding the initial potential risks, practice has shown that a high level of privacy concerns does not prevent people from disclosing their own personal information as perceived benefits often outweigh perceived risks [10]. Research on privacy suggests that private information disclosure is prevalent in modern society [3]. One of the key factors affecting privacy concerns is prior exposure to privacy breach. Typically, a breach occurs once the exchange relationship has been established and information has been shared, which is the case in many contexts nowadays. Since people may experience different privacy breach incidents, little is known about the factors that affect how such a breach is perceived. We take the first steps in addressing this knowledge gap by defining the construct of perceived privacy breach and examining the factors that influence privacy breach perceptions among smartphone application users.

We build our research model on the foundation of psychological contract theory. This theory posits that virtually all exchange relationships involve unwritten expectancies that comprise psychological contracts
Psychological contract theory predicts that multiple factors such as anticipated impact, attribution, salience and type of exchange affect the way in which psychological contract breach is perceived [23]. We conceptualize privacy-related expectancies as a core domain of psychological contracts associated with disclosure of private information.

We define perceived privacy breach as a perception that a privacy breach has taken place. On the basis of psychological contract theory, we investigate the factors influencing the perception that privacy has been breached and the severity with which the breach is perceived. To this end, we conduct two experimental studies to examine the effects of the type of information (financial, geolocation data) collected by smartphone applications, claims of legal rights to information in legal contracts which accompany the applications, the source of information suggesting that a privacy breach had occurred (the company or the media) and the type of the application (free or paid).

This study contributes to both theory and practice. Our key theoretical contribution is developing perceived privacy breach as a new focal construct for privacy-related research. While privacy concerns are critical at the beginning of exchange relationships, perceived privacy breach offers an opportunity to examine the impact of privacy infringements in ongoing information exchanges across different settings, such as social media and electronic medical record systems among other practically relevant contexts. Our key contribution to practice is in revealing that perceived privacy breach may occur even in the presence of a legal contract claiming rights to use the information. Therefore, application developers’ reliance on legal contracts does not preclude perceptions of privacy breach. While the legal contracts may give application developers legal rights to use information, they may not fully prevent conflicts arising from perceptions of privacy breach.

To describe this study, the next sections are structured as follows. First, we review prior research on privacy and develop the hypotheses underlying our research model. Next, we present the methodology and results. We conclude with a discussion of study limitations and our contributions to theory and practice.

2. Theory background and hypotheses

Privacy has been a topic of research in different disciplines spawning legal [34] and organizational studies [7], as well as information systems studies [24]. The legal definition of privacy was established by Warren and Brandeis [41] who defined privacy as “the right to be left alone.” This simple statement has evolved to generate a more precise legal definition in statutes and case law [34]. In the current study, we focus on information privacy which is defined as the individual ability to control personal information disclosure to others [42]. Instead of general privacy concerns, we focus on specific factors affecting perceptions of a privacy breach. To identify these factors, we draw from psychological contract theory.

Psychological contract theory evolved in the organizational context where researchers found that formal employment contracts had little predictive value in explaining employee performance and turnover intentions [28,29]. Psychological contract theory posits that virtually all exchange relationships involve unwritten expectancies which comprise psychological contracts [30]. A perceived breach of the expectancies (psychological contract breach) triggers attitudinal and behavioral adjustments [31].

While psychological contracts could have idiosyncratic aspects, some issues tend to be applicable to a broad range of people. For example, in the employment context, training, raises, and promotions are typical expectancies which form the basis of employment-related psychological contracts [29]. A perceived breach of these expectancies leads to reduced performance and increasing intentions to switch jobs [39]. Psychological contracts point to the limitations of legal contracts as a governance mechanism and provide a practically relevant perspective on sustainability of exchange relationships across different contexts. Psychological contract theory has been applied in Information Systems research in virtual teams [25], outsourcing [20] and online marketplaces [24]. Piccoli and Ives [26] found that apparent breach of expectancies among virtual team members had negative consequences on team performance. Koh et al. [21] found that fulfillment of psychological contracts was positively associated with success of outsourcing relationships. Pavlou and Gefen [25] found that apparent psychological contract breach among buyers in online marketplaces increased perceptions of risk and reduced intentions of future transactions. Taken together, the findings of these studies underscore the importance of psychological contracts in different technology-mediated contexts.

2.1. Hypotheses Development

Expectations of individual privacy are essential for the individual sense of dignity [27]. Perceptions of privacy breach affect individual sense of control
and have a negative impact on self-esteem and emotional well-being [9]. Private information disclosure enabled by technology presumes users’ expectations of privacy and trust in technology. Thus privacy-related expectancies comprise a core domain of psychological contracts associated with technology-enabled information disclosure. To put it differently, technology users expect their privacy to be respected and a perceived breach of privacy will constitute a breach of psychological contract. Therefore, we define perceived privacy breach as individual perceptions that privacy-related expectancies have been broken. A perceived privacy breach may occur even in the absence of an actual privacy breach because it depends on how users interpret the situation. Thus, in the case of an actual breach it is paramount to investigate how users perceive it. Since perceived privacy breach is the focal dependent variable in our study, we identify the factors that affect these perceptions.

The process model of psychological contract breach proposed by Morrison and Robinson [23] suggests that specific factors affect perceptions of a breach. They proposed that perceived breach is affected by: (1) the anticipated impact of breach, (2) the attribution of breach to either incongruence regarding the terms of agreement or reneging by the counterparty, (3) the salience of information suggesting breach, and (4) the type of exchange relationship. We evaluate the impact of these factors on perceptions of a privacy breach in a smartphone application context. Accordingly, we examine the effects of the type of information which may be misappropriated by smartphone applications, the claim of legal rights to information in legal contracts which accompany the applications, the source of information suggesting that a privacy breach may have occurred and the effect of application cost.

The first factor is the type of information which may be misappropriated by smartphone applications. Smartphones act as an important conduit for information sharing and expose the smartphone users to a broad range of potential privacy violations. Among all the possible types of personal information that could be the subject of privacy breaches, the misuse of financial information and/or geo-location data has the most potential for causing negative consequences such as financial damages and threats to personal security.

A recent survey of mobile users’ suggests that transactions involving financial information (banking, online shopping) are perceived to pose the greatest risk to mobile users’ privacy [38]. Clearly, a potential breach of financial privacy exposes mobile users to loss or privacy as well as to potential financial losses. Another common concern among mobile users, which has received much attention among practitioners and researchers, is the disclosure of smartphone users’ geo-location information [16,43]. Virtually all smartphones are equipped with global positioning technologies which allow the devices to pin point users’ locations. This functionality facilitates location-based services, for example navigation and local search. While geo-location functions embedded in the smartphones offer practical utility, they can also be used for continuous monitoring of mobile users’ locations thus posing a threat to privacy. Location-based services received increasing attention after a researcher reported that Apple’s iPhone devices stored a history of locations visited by device owners without offering any notice or an opportunity to opt-out [40]. Psychological contract theory predicts that the expected impact of the type of information misused will be positively related to perceptions of breach. In other words, a perceived breach which threatens to do more damage will trigger higher perceptions of privacy breach. Disclosures of location-related and financial information both pose potential privacy risks for mobile users, but perceived breach of private financial information additionally exposes users to potential financial risk. Therefore, we expect that:

H1. Perceived misappropriation of financial information will cause higher perceptions of privacy breach compared to perceived misappropriation of geo-location data.

Perceptions of a psychological contract breach trigger a process of sense-making by the affected individuals. In this process, another key factor affecting the extent of perceived breach is whether the breach occurred due to willful reneging or due to incongruence of beliefs regarding the terms of the relationship among the parties. Rousseau [30] noted that psychological contracts and legal contracts may co-exist and differ substantially in terms. Morrison and Robinson [23] predicted that willful reneging will be associated with greater perceptions of psychological contract breach compared to incongruence of beliefs regarding the terms between the parties. The legal terms of the relationships between smartphone application users and the application developers are commonly detailed in user agreements which typically accompany the applications. Users have to accept the terms prior to using the application. The legal agreements are often very broad (and long) and include comprehensive claims of rights in relation to information that users provide. For example, Instagram, a popular social
media application, includes the following among the terms of service: “you hereby grant to Instagram a non-exclusive, fully paid and royalty-free, transferable, sub-licensable, worldwide license to use the Content that you post on or through the Service” [18]. Although users typically fail to read in detail the legal contracts online [13], we expect that the presence of legal claims related to information shared by application users will lead to perception of incongruence among application users, and therefore claims of legal rights will partially reduce perceptions of privacy breach. In other words, we expect that contractual claims of legal rights to users’ private information which accompany smartphone applications will reduce perceptions of privacy breach among smartphone users.

**H2.** The presence of legal rights claims in the user agreement contracts will reduce perceptions of a privacy breach compared to the absence of such claims.

Users’ reactions to new information suggesting that a privacy breach may have occurred will also be affected by how users’ process this information. Attribution theory predicts that information salience is influenced by evaluation of the source of information [20]. Expert sources are generally perceived as more credible than general news media and people often ignore news sources that they do not perceive as credible [1]. Further, information recipients seek to understand the motivations of the party communicating information. For example, negative earnings warnings by publicly traded companies are often seen as actions meant to limit management liability for timely disclosure of material information which is required by financial regulation [32]. In the case of computer-related breaches, earlier research has found that the market differentiates across types of breaches and reacts more negatively when confidential data is compromised [6]. We expect that the salience of information suggesting that a privacy breach may have occurred will be processed depending upon the source providing the information and the possible motivations. A study on the impact of software vulnerability reports that investors perceive more negatively such disclosures when they are released by the software companies themselves, instead of third-parties [35]. Usually, the affected company has access to more precise information about the nature of the breach and the extent of the impact than external sources (i.e. press), which typically rely on anecdotal evidence. Accordingly, a voluntary disclosure of a privacy breach originating from the developer of smartphone applications will be perceived as more severe than general media reports and it will be associated with higher level of perceived privacy breach.

**H3.** Reports of a privacy breach by companies would be more strongly associated with perceptions of a privacy breach than reports by the media.

The fourth factor is whether the smartphone application at the center of the privacy breach is paid or free. The use of smartphone applications is an exchange relationship. If the use of a smartphone application requires payment then the exchange is economic. In economic exchanges payment is traded for expected benefits associated with the use of the application. In contrast, when the application is free the exchange is non-economic. Economic exchanges typically carry more clearly defined expectancies compared to non-economic exchanges [37]. Non-economic exchanges are governed by the rules of reciprocity [15]. However, in the context of free smartphone applications it may not always be clear what the users are trading for a free application. Provided that economic exchanges generally carry more clearly defined expectancies in terms of psychological contracts, we expect that a perceived privacy breach by a paid application will be perceived to be more severe compared to a perceived privacy breach attributed to a free application.

**H4.** Perceptions of a privacy breach will be higher for paid apps compared to free apps.

Figure 1 summarizes our research model.
3. Methodology

In order to investigate the factors associated with a privacy breach, the manipulations were implemented through vignettes. These are short descriptions of hypothetical situations or events, which are widely used in the study of perceptions, attitudes or beliefs [8]. Vignettes provide a common frame of reference or situation to compare perceptions. Vignette-based studies are valid and reliable, and reach the same conclusions as non-vignette studies [8].

To design the empirical study, we considered alternative options for the manipulation of the four factors. We decided against a full factorial design due to the high number of conditions (16), and the number of interaction effects with subsets of factors for which we did not have theoretical basis to formulate hypotheses. We also discarded the alternative of manipulating one factor at a time due to the simplicity of the associated vignettes. Additionally, earlier pilot studies indicated that participants can reliably recall only two factors in the vignettes. For these reasons, we conducted two 2x2 factorial experiments.

The manipulation of two factors at a time enabled us to reduce the number of conditions, design more complete vignettes and retain the ability to explore some interaction effects. The two factor pairs were selected such that one set of factors was descriptive of the breach (type of information misused and claims in the legal contract), while the other set of factors affected salience of information related to the exchange (source of information that a breach occurred and cost of the application). The pairings for the factorial designs were selected such that there was a breach descriptor (type of information or source of news) and an app feature (legal claims or application cost) in each experiment.

In each study, participants were randomly assigned to one of the four experimental conditions and presented with the corresponding vignette. Each vignette described a smartphone application and suggested that the application may have misappropriated private information. The text of the vignettes is provided in the appendix.

In the first experiment, we manipulated the type of information which was misappropriated by the application (financial data versus geo-location data) and the presence of legal claims in relation to information appropriated by the application (present versus not present in the legal contract). In the second experiment, we manipulated the source of information suggesting a privacy breach may have occurred (company or media) and the type of exchange (paid versus free application). Treatment conditions are summarized in Table 1.

<table>
<thead>
<tr>
<th>Experiment 1 (Type of information and Claims in legal contract)</th>
<th>Experiment 2 (Source of privacy breach news and Application cost)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition 1: Event Apps Geo-location data and legal rights claimed in legal contract</td>
<td>Condition 1: News media source and free app</td>
</tr>
<tr>
<td>Condition 2: EZBanking Financial data and legal rights claimed in legal contract</td>
<td>Condition 2: Company source and free app</td>
</tr>
<tr>
<td>Condition 3: Event Apps Geo-location data and legal rights not claimed in legal contract</td>
<td>Condition 3: News media source and paid app</td>
</tr>
<tr>
<td>Condition 4: EZBanking Financial data and legal rights not claimed in legal contract</td>
<td>Condition 4: Company source and paid app</td>
</tr>
</tbody>
</table>

The dependent variable in both studies is the perception of a privacy breach. We used two measures to evaluate perceived privacy breach. First, we asked the study participants to indicate if they believed the application described in the vignette violated users’ privacy. This provided a binary categorical measure of perceived privacy breach (hereafter called PPBBin). Second, we asked the study participants to indicate how significant the privacy breach was using a continuous rating scale 0-100, 0 – not at all significant, 100 – extremely significant (hereafter called PPBSig). Our choice of 0-100 scale is grounded in prior research in psychology which suggests that 0-100 scales often have better psychometric properties compared to narrow range scales [2]. We used the binary and ratio measures to evaluate between group differences in perceptions of privacy breach.

Participants for the study were recruited from the undergraduate student population of a large university in the northeastern United States. They received academic credit towards an introductory course in information systems in exchange for participation in the study. The use of students as subjects is justified in the current study because students are among the most active smartphone users [4]. Industry statistics indicate that smartphone

Figure 1. Research model
adoption among young adults has reached over 69% compared to 44% for general population [5]. To assure ecological validity of the study, we required the participants to have prior smartphone use experience. Participants in the study were provided with a link to the survey which automatically assigned participants to one of the treatment conditions. The survey collected basic demographic variables (age, gender and the length of smartphone use), exposed the participants to the corresponding vignette containing the experimental manipulation, and collected their responses related to perceived privacy breach. We also included manipulation checks to ensure that participants read carefully and understood the vignettes. The checks were implemented as questions asking participants to recall specific details of their assigned vignettes.

4. Results

In the first experiment, we manipulated the type of information collected by the application (geo-location data versus financial information) and the content of the legal contract which accompanied the application (legal contract claims legal rights in relation to the data versus legal contract does not explicitly claim legal rights). We recruited 157 participants for this experiment. After examining manipulation checks, we excluded 29 responses from participants that did not read the vignettes carefully. This left us with a sample of 128 responses. The results are summarized in Table 2.

| Table 2. Information type and legal claims’ effects on perceived privacy breach |
|---------------------------|---------------------------|
| Events App                | EZ Banking App            |
| **Legal contract claims rights to information** | **Legal contract' claims rights to information** |
| Condition 1               | Condition 2               |
| N = 30                    | N = 32                    |
| PPBBin: 77.4% (SD = 7.6%) | PPBBin: 88.6% (SD = 5.6%) |
| PPBSig: 64.4 (SD = 24)    | PPBSig: 79.9 (SD = 21)    |
| Condition 3               | Condition 4               |
| N = 31                    | N = 35                    |
| PPBBin: 96.7% (SD = 3.2%) | PPBBin: 93.8% (SD = 4.1%) |
| PPBSig: 72.1 (SD = 20)    | PPBSig: 86.7 (SD = 14)    |

To evaluate the main effects of information type and legal claims, we dummy-coded treatment conditions as follows: 0 – Events app, 1 – EZ banking app; 1 – legal rights claimed in the legal contract, 0 – no claim of legal rights in the contract. We used a linear regression model to estimate treatment effects on the perceived significance of privacy breach. The regression model was significant (F(2,125) = 10.75, p<0.001). We found significant main effects for the type of information which was misappropriated (b = 15.05, p < 0.001) and the claim of legal rights in the legal contract which accompanied the application (b = -7.23, p < 0.05). No interaction effects were present. The results provide support for H1 and H2. Perceived misappropriation of financial information is perceived as a more significant type of privacy breach compared to misappropriation of geo-location data. Since the coefficient is negative and significant, the claim of legal rights in the legal contract partially ameliorates the degree of perceived privacy breach. The results are graphically presented in Figure 2.

Figure 2. Information type and legal claims’ effects on perceived privacy breach

In the second experiment, we manipulated the cost of application (paid or free), and the source of information suggesting that a privacy breach may have occurred (general news outlets such as TV, newspapers versus the company which made the application). We recruited 135 participants for the second experiment. After examining manipulation checks, we excluded 26 responses because the participants did not read carefully the vignettes. This left us with a sample of 109 responses. The results are summarized in Table 3.

| Table 3. Source of information and cost of application effects on perceived privacy breach |
|-----------------------------------------------|---------------------------|
| Events App                                  | EZ Banking App            |
| **Legal contract claims rights to information** | **Legal contract' claims rights to information** |
| Condition 1                                 | Condition 2               |
| N = 30                                      | N = 32                    |
| PPBBin: 77.4% (SD = 7.6%)                    | PPBBin: 88.6% (SD = 5.6%) |
| PPBSig: 64.4 (SD = 24)                       | PPBSig: 79.9 (SD = 21)    |
| Condition 3                                 | Condition 4               |
| N = 31                                      | N = 35                    |
| PPBBin: 96.7% (SD = 3.2%)                    | PPBBin: 93.8% (SD = 4.1%) |
| PPBSig: 72.1 (SD = 20)                       | PPBSig: 86.7 (SD = 14)    |

We dummy-coded treatment conditions as follows: 0 – media, 1 – company; 0 – free app, 1 – paid app. We used linear regression to evaluate main effects of the source of information suggesting privacy breach (news media versus the company) and the application type (free versus paid) on perceived significance of privacy breach. The regression model
was not significant (F(2,106)=1.65; p=0.198). Neither of the main effects was found to be significant at the 0.05 level. We further examined between group differences in fractions of respondents indicating a privacy breach by evaluating individual inter-group differences, but we found no statistical support for either of the main effects. Therefore, H3 and H4 are not supported.

Table 3. Application cost and information source effects on perceived privacy breach

<table>
<thead>
<tr>
<th>Source of information: news media</th>
<th>Source of information: the company which made the application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free Application</td>
<td></td>
</tr>
<tr>
<td>Condition 1</td>
<td>N = 29</td>
</tr>
<tr>
<td>PBBin: 82.8% (SD = 7%)</td>
<td>PBBin: 92.6% (SD = 5%)</td>
</tr>
<tr>
<td>PPBSig: 76 (SD = 29.6)</td>
<td>PPBSig: 84.1 (SD = 15.8)</td>
</tr>
<tr>
<td>Condition 2</td>
<td>N = 27</td>
</tr>
<tr>
<td>PBBin: 92.6% (SD = 5%)</td>
<td>PPBSig: 84.1 (SD = 15.8)</td>
</tr>
<tr>
<td>Paid Application</td>
<td></td>
</tr>
<tr>
<td>Condition 3</td>
<td>N = 28</td>
</tr>
<tr>
<td>PBBin: 89.3% (SD = 5.8%)</td>
<td>PBBin: 92% (SD = 5.4%)</td>
</tr>
<tr>
<td>PPBSig: 85.5 (SD = 15.5)</td>
<td>PPBSig: 85.5 (SD = 15.5)</td>
</tr>
<tr>
<td>Condition 4</td>
<td>N = 35</td>
</tr>
<tr>
<td>PBBin: 92% (SD = 5.4%)</td>
<td>PPBSig: 85.5 (SD = 15.5)</td>
</tr>
</tbody>
</table>

5. Discussion

Privacy remains a topic of active discussion among practitioners, researchers and legislators. In this study, we examine factors that affect the perceptions of severity of a privacy breach. To this end, we draw on psychological contract theory which posits that virtually all exchange relationships involve a set of unwritten expectancies which comprise psychological contracts, and we propose that privacy-related expectancies are inherent to private information disclosure. In this context, a perceived breach of privacy-related expectancies constitutes a breach of psychological contract. We developed and operationalized the perceived privacy breach construct and examined specific factors affecting perceptions of a privacy breach among smartphone application users.

We conducted two experimental studies and we used vignettes to operationalize treatment conditions. The first study examined the separate and joint effects of the type of personal information breached (financial versus geo-location data) and the claim of rights in the legal contracts which accompany the applications. We found significant main effects for the type information and the presence of information rights claims in the legal contracts. Perceived breach of privacy involving financial information causes higher perceptions of privacy breach compared to geo-location data. In addition, the presence of legal claims to use the information in the legal contracts partially reduces perceptions of a privacy breach.

The second study investigated the source of information suggesting that a privacy breach may have occurred and the cost of the application (paid, free) on perceptions of a privacy breach. We found no support for the effects of application cost or source of information.

Several possible explanations may account for the lack of support for the hypotheses related to news source and application cost. One possibility is that the factors involved (news source of a breach and cost of the application) are not salient enough to significantly affect the intensity of privacy breach perceptions. Bounded rationality affects human information processing and decision making [19]. Faced with cognitive constraints people act as cognitive misers and extract the most salient factors from available information [36]. Our manipulation checks support this explanation. In both experiments, we asked the participants to rank order the four factors according to their importance in the perceptions of privacy breach. The same rank order of factors emerged from all treatment conditions across both experiments. Collection of information by the application was ranked as the top concern, followed by the details of the legal contract. The price of smartphone application was ranked third and the source of information was ranked last. In other words, the two most important factors in assessing privacy breach by smartphone applications users are the type of personal information collected by the application and the claim of rights in the legal contracts.

A second possible explanation for the lack of support for hypotheses 3 and 4 is that the selection of context (smartphone application usage) reduces the relevance of these two factors. If the effects of these two factors exist but in smaller magnitude, a much larger sample size would have been needed to detect them. While the cost of application and the source of privacy breach information may play a role, further research is necessary to investigate these alternative explanations.

Our study makes a number of contributions to theory and practice. Our first contribution to theory is the development and operationalization of perceived
privacy breach as a new construct for privacy research. Aside from general privacy concerns, which has been the subject of prior research, perceived privacy breach offers the opportunity to examine the impact of privacy breach perceptions in ongoing information exchanges. In developing the construct, we integrated research on privacy and psychological contract theory pointing to a novel theoretical perspective to guide privacy-related research.

This study also makes a contribution to practice. Our findings reveal that legal contracts, which commonly provide the foundation for the claims of rights in relation to information shared by technology users, do not prevent perceptions of a privacy breach. However, these claims do contribute to reduce the severity of the perceptions associated with the breach. For these reason, claim of rights in the legal contracts do matter. In addressing growing consumer privacy concerns, the Federal Trade Commission recently called for clearer articulation of legal claims in legal contracts [14]. However, it appears that legal contracts are limited in their ability to prevent breaches and a broader regulatory action may be required to address smartphone users’ concerns over privacy.

The limitations of our study stem from reliance on student subjects. While students are among the most active smartphone users, they nonetheless represent a narrow demographic sample and therefore further research would be needed to assess generalizability of our findings. Further, although we maximized ecological validity in our experimental treatments, they may not reflect the complexity of privacy-related perceptions influencing smartphone users in a real-life context. Yet another limitation of our study is that we did not employ a full factorial design due to a large number of participants that would be required to examine all possible combinations of factors. Therefore it is possible that some factor interaction effects were not detected in our experiments, particularly between other breach and company characteristics such as type of info misused and cost of the application. These limitations point to opportunities for further research. Natural field experiments with a broader demographic sample employing a full factorial design would be likely to reveal a more complex milieu of factors affecting privacy perceptions.

6. Conclusion

The current study explores factors contributing to perceptions of privacy breach among smartphone application users. We draw on psychological contract theory and we experimentally evaluate the effects of the type of information misappropriated by the application, the presence of legal claims of rights to information, the cost of application and the source reporting a possible privacy breach on users’ perceptions of privacy breach. Our results indicate perceived misappropriation of financial information is perceived as a more severe type of privacy breach than perceived misappropriation of geo-location data. The existence of a legal contract giving rights to information to the application developer only partially reduces perceptions of privacy breach. Our findings offer contributions to both theory and practice. We develop perceived privacy breach as a novel construct for privacy research and our results point to the limited utility of legal contracts in mitigating perceptions of privacy breach.

7. References


Accountants. The app works in their bank accounts. A banking app recently users had to accept prior to users had to accept prior to users have to accept upon personal and personal and location information about the individual users. It is unclear how the information was gathered. Wall Street Journal, 2011. http://online.wsj.com/article/SB10001424052748704123204576283580249161342.html.


9. Appendix Vignettes

Experiment 1

Condition 1.
Events app is a popular free app used by many smartphone owners to find out about local events. The company which makes Events app recently notified the app users that Events app gathered geo-location information about the individual users'. It is unclear how the information was used. The existing legal agreement which users had to accept prior to using Events app gave the company the right to capture personal information about the individual users.

Condition 2.
EZ Banking is a popular free app. It is used by many smartphone owners to check balances in their bank accounts. The app works with most commercial banks. The company which makes EZ Banking app recently notified the app users that EZ Banking app gathered personal and financial information about the users'. The information was sold to credit agencies and other financial institutions. The existing legal agreement which users had to accept prior to using EZ Banking gave the company the right to capture personal and financial information about the individual users.

Condition 3.
Events app is a popular free app used by many smartphone owners to find out about local events. The company which makes Events app recently notified the app users that the application gathered geo-location information about the users’. It is unclear how the information was used. The existing legal agreement which users have to accept upon purchasing Events app did not specify whether the company had the right to capture geo-location information about the individual users.

Condition 4.
EZ Banking is a popular free app. It is used by many smartphone owners to check balances in their bank accounts. The app works with most commercial banks. The company which makes EZ Banking app recently notified the app users that EZ Banking app gathered personal and financial information about the users’. The information was sold to credit agencies and other financial institutions. The legal agreement which users have to accept upon purchasing EZ Banking app did not specify whether the company had the right to sell personal and financial information about the individual users.

Experiment 2

Condition 1.
EZ Banking is a popular free app. It is used by many smartphone owners to check balances in their bank accounts. The app works with most commercial banks. The company which makes EZ Banking app recently notified the app users that EZ Banking app gathered personal and financial information about the users’. The information was sold to credit agencies and other financial institutions. The legal agreement which users have to accept upon purchasing EZ Banking app did not specify whether the company had the right to sell personal and financial information about the individual users.

Condition 2.
EZ Banking is a popular free app. It is used by many smartphone owners to check balances in their bank accounts. The app works with most commercial banks. The company which makes EZ Banking app recently notified the app users that EZ Banking app gathered personal and financial information about the users’. The information was sold to credit agencies and other financial institutions. The legal agreement which users had to accept prior to using EZ Banking gave the company the right to capture personal and financial information about the individual users.

Condition 3.
EZ Banking is a popular paid app which costs $2.99. It is used by many smartphone owners to check balances in their bank accounts. The app works with most commercial banks. News media (newspapers and TV networks) recently reported that EZ Banking app gathered personal and financial information about the users’. The information was sold to credit agencies and other financial institutions. The existing legal agreement which users had to accept prior to using EZ Banking gave the company the right to capture personal and financial information about the individual users.

Condition 4.
EZ Banking is a popular paid app which costs $2.99. It is used by many smartphone owners to check balances in their bank accounts. The app works with most commercial banks. The company which makes EZ Banking app recently notified the app users that EZ Banking app gathered personal and financial information about the users’. The information was sold to credit agencies and other financial institutions. The existing legal agreement which users had to accept prior to using EZ Banking gave the company the right to capture personal and financial information about the individual users.