12-12-2021

Privacy policy violations: A corporate nexus of healthcare providers and social media platforms

John R. Drake
East Carolina University, drakejo@ecu.edu

Christopher P. Furner
East Carolina University

Nikhil Mehta
University of North Carolina Greensboro

Privacy Policies Violations: A Corporate Nexus of Healthcare Providers and Social Media Platforms

John R. Drake[1]
College of Business, East Carolina University,
Greenville, NC, USA

Christopher P. Furner
College of Business, East Carolina University,
Greenville, NC, USA

Nikhil Mehta
Bryan College of Business and Economics, UNC Greensboro,
Greensboro, NC, USA

ABSTRACT

When healthcare information is shared on social media, who's to blame? It can be difficult for users to determine whether it was the social media platform or the healthcare provider that caused the privacy violation. A model of behavioral intentions following a privacy breach on a social media platform is developed in which perceptions of psychological contract violations for both entities determine multiple response intentions.

Keywords: privacy, psychological contract violation, social media, healthcare, policy violations

INTRODUCTION

Privacy is a desired state in which an individual is protected from intrusion, interference, and information access by others (Drake 2016), and has been a primary domain of information systems research since the emergence of field (Turn and Ware 1976). As the amount of information shared on social media increases, privacy concerns of users are becoming increasingly paramount. Companies develop and publish privacy policies to inform users of the

[1] Corresponding author. drakejo@ecu.edu +1 252 737 4566

information that they collect and how it is used. Privacy policies serve as an assurance to users that their information will be used and shared in delimited and respectful ways (Xu et al. 2011). Presumably, these privacy policies assuage the major concerns of most of their users.

Whether or not privacy policies are legally enforceable, consumers construe them as an implied contract between the user and the company (Pan and Zinkhan 2006). So, when privacy is breached, users feel as if a contract between them and the company has been violated. This can result in a psychological reaction by users and a potential privacy policy disaster (Culnan 2019). While some studies have explored the effects of unintentional privacy breaches on users' psychological contract violations (PCV) (Choi et al. 2016), there's a gap in understanding how intentional policy violations impact PCV, particularly where healthcare information is shared on a social media platform. It can be difficult for individuals to determine which entity, a healthcare provider or a social media platform, is responsible for a privacy violation. It is also unclear how different privacy violation types will impact these perceptions.

> RQ1: When a perceived privacy violation occurs, does the content of the privacy policy and violation type influence consumers' construal of the violation of psychological contract?
>
> RQ2: In a social media and healthcare nexus, does the privacy policy of one entity influence the construal of a violation of psychological contract related to the other entity?
>
> RQ3: How do consumer's perceptions of privacy violations influence their behavioral intentions toward the entities involved?

LITERATURE REVIEW

To answer these research questions, literature related to privacy policies, PCV and responses to privacy violations are reviewed, and a model is developed which examines the effectiveness of privacy policy on PCV and response intentions.

Privacy Policies

Privacy policies are statements which describe a firm's data collection, use and disclosure practices (Earp et al. 2005). They inform consumers or other individuals who interact with the firm about what data they will collect, the ways in which that data will be used and under what conditions that data will be shared with third parties. These policies usually provide guidance on the capabilities that consumers have to control the collection use and distribution of their data.

Since privacy policies have the goal of empowering users to make informed decisions, and have the effect of shielding firms from liability, some researchers have questioned the efficacy of privacy policies in informing consumers. For example, Jafar and Abdullat (2009) found that to properly understand a typical 2009 privacy policy, readers would need a minimum of two years of college education. They note that 60% of social media users read at a grade level of 5 or below, making it difficult for consumers to understand those policies. Yet, Keith et al. (2013) found that when a mobile location based service provides a privacy assurance, consumer perceptions of risks are lower, and both adoption and willingness to pay for the service increase.

When these policies fail, legal action may be necessary. Legal doctrine suggests there are four invasion of privacy torts, 1) intrusion of solitude, 2) appropriation of name or likeness, 3) public disclosure of private facts, and 4) false light (Prosser 1978). Intrusion of solitude involves intentionally prying into a person's private information or seclusion. With appropriation of name or likeness, a defendant claims that their identity was used in an exploitive manner without consent. In public disclosure of private facts, a defendant claims that private facts were disclosed in a public forum that a reasonable person would consider offensive. False light is similar to defamation but less stringent in that it claims that personal information about the defendant portrays them in a false or misleading light deemed offensive.

Psychological Contract Violations

While privacy policies imply a contract, individuals develop subjective expectations of behavior within a social context (Serino et al. 2005). Robinson (1996) notes that these expectations are construed and exist in the mind of the individual and may not be explicitly agreed upon. Consequentially, even when a privacy policy explicitly empowers an entity to take an action, it's possible that an individual will form an expectation that the entity should not take that action, particularly if the action may cause harm to the individual.

Privacy researchers have tied PCVs to a variety of individual attitudes and intentions. Cistulli and Snyder (2019) investigated situations in which supervisors were connected to employees via social media. A survey of employees measured perceptions of supervisor trust, social media privacy, violations of psychological contract and affective organization commitment. They found that perceptions of social media privacy explained approximately 50% of the variance in supervisor trust. They also supported a negative relationship between PCVs and organizational commitment. Choi et al. (2016) examined consumer attitudes about firms which had been affected by a privacy breach and modeled the influence of the firm's actions following the breach on word of mouth and switching intentions. The researchers used services recovery theory to support their model, and central to the development of their hypotheses were justice theory and psychological contract theory. They found that perceptions of justice are significantly related to PCVs, and that perceptions of violations influenced word-of-mouth intentions as well as switching intentions.

Information Privacy Protective Responses

When privacy is threatened, users engage in information privacy protective responses (Son and Kim 2008). Users may instantiate different responses when attempting to protect one's

privacy, either before a violation or in response to one. These responses found saliency in intrusion of solitude contexts, when human resource professionals screened job candidates by requesting social media login information (Drake et al. 2016), with differing response profiles across cultures (Sun et al. In press).

MODEL DEVELOPMENT

A model of responses to privacy violations is developed in which PCVs mediate the relationships between privacy concerns, perceptions of the privacy policy effectiveness and response intentions. The research model is presented in Figure 1.

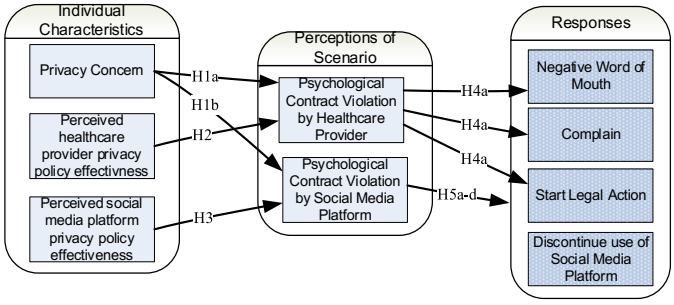

Figure 1: Research Model

According to Robinson (1996), individuals perceive PCVs when the behavior of another entity does not conform to their construal of agreed upon behavioral expectations. Privacy concerns are tied to uncertainty about the harm that may result from the disclosure of information, with those who score higher in privacy concern experiencing a stronger desire for harm avoidance (Anic et al. 2019). As such, we propose that individuals who report higher levels of privacy concern will be more apprehensive about the harm that might stem from a privacy violation and will thus increase perceived PCV. We believe that this will be the case for both the social media platform and for the health care provider.

H1a-b: Privacy concerns will increase perceptions of PCVs of each company

Privacy policies vary in the extent to which the foster a sense of security and protection from harm (Pollach 2007), and individuals differ in the extent to which the perceive security and protection from harm based on a given policy (Chang et al. 2018). Chang et al. (2018) found that when consumers perceive that a privacy policy is effective, they report higher levels of privacy control and lower levels of perceived risk, suggesting a reduced expectation of harm. We predict that when an individual experiences privacy harm, their construal of PCV will be higher when they perceive that the privacy policy was effective. That is, since consumers who perceive a privacy policy to be effective expect to experience less harm, these consumers will have a stronger reaction to the harm that accompanies a privacy violation, thus resulting in a stronger perception of PCV.

H2-3: Perceived effectiveness of the privacy policies will increase PCV of each company

When a privacy violation occurs, individuals may adopt a mix of responses (Drake et al. 2016). The reaction to PCV can leave an individual feeling cheated and exploited, which we predict will trigger two responses. First, justice theory suggests that individual may seek to rectify the loss by complaining to the parties which the individual attributes to the violation, and even initiating legal action (Choi et al. 2016). Second, the individual will seek to mitigate any future damage by discontinuing use of the social media platform, and to warn others via negative word of mouth (Son and Kim 2008).

H4a-c: When PCV by the healthcare provider is high, negative word of mouth intention, intention to complain and intention to start legal action will increase.

H5a-d: When PCV by the social media platform is high, negative word of mouth intention, intention to complain intention to start legal action and intention to discontinue use of the social media platform will increase.

METHODOLOGY

This study will use an experimental vignettes methodology with between-subject design. Participants will be asked to read two privacy policies, one from a healthcare provider and one from a social media platform. The healthcare context was selected because healthcare privacy violations are expected to elicit a strong enough response to motivate subjects. Both policies will be modified to remove identifying information and remove legal jargon (see appendix A). After viewing each policy, participants will be asked about the perceived effectiveness of each policy.

Participants will then be provided with a vignette that describes a situation where personal information from a healthcare provider is shared on a social media platform, eliciting a potential PVC by either the healthcare provider or the social media platform or both. Given that violation, participants then identify which privacy protective responses they might use. The vignettes are based on legal cases of four types of privacy violations: intrusion of solitude, appropriation of name or likeness, public disclosure of private facts, and false light. The vignettes were vetted by a panel of experts and a pilot study of 76 participants. A final version can be found in Appendix B. To measure antecedents and reactions to the vignettes, constructs in this study will be adapted from existing measures: information privacy-protective responses (Son and Kim 2008). PCVs measures (Suazo 2009), privacy concern (Malhotra et al. 2004), and perceived effectiveness of the privacy policy (Xu et al. 2011).

Data will be collected from two sources, 1) approximately 200 students from multiple universities in the US and 2) approximately 600 participants from a US general population, obtained through Prolific, a survey company. This will result in approximately 800 participants, roughly 200 participants per vignette. Students will be offered extra credit for participation and the Prolific sample will be offered $5 for participation.

REFERENCES

Anic, I.-D., Budak, J., Rajh, E., Recher, V., Skare, V., and Skrinjaric, B. 2019. "Extended Model of Online Privacy Concern: What Drives Consumers' Decisions?," *Online Information Review* (43:5), pp. 799-817.

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., and Lee, H. 2018. "The Role of Privacy Policy on Consumers' Perceived Privacy," *Government Information Quarterly* (35:3), pp. 445-459.

Choi, B. C. F., Kim, S. S., and Jiang, Z. 2016. "Influence of Firm's Recovery Endeavors Upon Privacy Breach on Online Customer Behavior," *Journal of Management Information Systems* (33:3), pp. 904-933.

Cistulli, M. D., and Snyder, J. L. 2019. "Privacy in Social Media Friendships with Direct Supervisors: A Psychological Contract Perspective," *International Journal of Business Communication*), p. 2329488419856072.

Culnan, M. J. 2019. "Policy to Avoid a Privacy Disaster," *Journal for the Association of Information Systems* (20:6), pp. 848-856.

Drake, J. R. 2016. "Asking for Facebook Logins: An Egoist Case for Privacy," *Journal of Business Ethics* (139:3), pp. 429-441.

Drake, J. R., Hall, D. J., Becton, B., and Posey, C. 2016. "Job Applicants' Information Privacy Protection Responses: Using Social Media for Candidate Screening," *AIS Transactions on HCI* (8:4), pp. 160-184.

Earp, J. B., Antón, A. I., Aiman-Smith, L., and Stufflebeam, W. H. 2005. "Examining Internet Privacy Policies within the Context of User Privacy Values," *IEEE Transactions on Engineering Management* (52:2), pp. 227-237.

Jafar, M. J., and Abdullat, A. 2009. "Exploratory Analysis of the Readability of Information Privacy Statement of the Primary Social Networks," *Journal of Business & Economics Research (JBER)* (7:12).

Keith, M. J., Babb, J., Lowry, P. B., Furner, C., and Abdullat, A. 2013. "The Roles of Privacy Assurance, Network Effects, and Information Cascades in the Adoption of and Willingness to Pay for Location-Based Services with Mobile Applications," in: *Dewald Roode Informaiton Security Workshop*.

Malhotra, N. K., Kim, S. S., and Agarwal, R. 2004. "Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336-355.

Pan, Y., and Zinkhan, G. M. 2006. "Exploring the Impact of Online Privacy Disclosures on Consumer Trust," *Journal of retailing* (82:4), pp. 331-338.

Pollach, I. 2007. "What's Wrong with Online Privacy Policies?," *Communications of the ACM* (50:9), pp. 103-108.

Prosser, R. A. 1978. "The Right to Privacy," *Georgia Law Review* (12:3), pp. 393-422.

Robinson, S. L. 1996. "Trust and Breach of the Psychological Contract," *Administrative Science Quarterly* (41:4), pp. 574-599.

Serino, C. A., Furner, C. P., and Smatt, C. 2005. "Making It Personal: How Personalization Affects Trust over Time," *Proceedings of the 38th Hawaii International Conference on System Sciences*, Waikaloa, HI: IEEE.

Son, J.-Y., and Kim, S. S. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), pp. 503-529.

Suazo, M. M. 2009. "The Mediating Role of Psychological Contract Violation on the Relations between Psychological Contract Breach and Work-Related Attitudes and Behaviors," *Journal of Managerial Psychology* (24:2), pp. 136-160.

Sun, S., Drake, J. R., and Hall, D. In press. "When Job Candidates Experience Social Media Privacy Violations: A Cross-Culture Study," *Journal of Global Information Management*).

Turn, and Ware. 1976. "Privacy and Security Issues in Information Systems," *IEEE Transactions on Computers* (C-25:12), pp. 1353-1361.

Xu, H., Dinev, T., Smith, J. H., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12:12), pp. 798-824.

APPENDIX A – PRIVACY POLICIES

HEALTHCARE PRIVACY POLICY

We are required by law to protect the privacy of your health information. We are also required to send you this notice, which explains how we may use information about you and when we can give out or "disclose" that information to others. You also have rights regarding your health information that are described in this notice. We are required by law to abide by the terms of this notice.

How We Use or Disclose Information

We must use and disclose your health information to provide that information:

- To you or someone who has the legal right to act for you; and
- To the Secretary of the Department of Health and Human Services.

We have the right to use and disclose health information for your treatment, to pay for your health care and to operate our business. For example:

- For Payment of premiums due us.
- For Treatment.
- For Health Care Operations.
- To Provide You Information on Health Related Programs or Products.
- For Plan Sponsors.
- For Underwriting Purposes.
- For Reminders.

We may use or disclose your health information for the following purposes under limited circumstances:

- As Required by Law.
- To Persons Involved With Your Care.
- For Public Health Activities such as reporting or preventing disease outbreaks.
- For Reporting Victims of Abuse, Neglect or Domestic Violence.
- For Health Oversight Activities.
- To Avoid a Serious Threat to Health or Safety to you, another person, or the public.
- For Specialized Government Functions.
- For Research Purposes.
- For Organ Procurement Purposes.
- To Business Associates.

What Are Your Rights

- The following are your rights with respect to your health information:
- To ask to restrict uses or disclosures of your information for treatment, payment, or health care operations.
- To ask to receive confidential communications.
- To see and obtain a copy of certain health information.
- To ask to amend certain health information.
- To receive an accounting of certain disclosures of your information.
- To a paper copy of this notice.

SOCIAL MEDIA PRIVACY POLICY

Welcome to the "Platform". We are committed to protecting and respecting your privacy.

What information do we collect?

We collect information when you create an account and use the Platform, when you share with us from third-party social network providers, and when information contained in the messages is sent through our Platform.

Information you choose to provide

- Registration information
- Profile information, such as name, social media account information, and profile image
- User-generated content,
- Payment information, such as PayPal or other third-party payment
- Your phone and social network contacts, with your permission.
- Your opt-in choices and communication preferences
- Information to verify an account
- Information in correspondence you send to us
- Information you share through surveys or your participation in challenges, sweepstakes, or contests.

Information we obtain from other sources

- Social Media
- Third-Party Services
- Others Users of the Platform
- Other Sources

Information we collect automatically

- Usage Information
- Device Information
- Location data
- Messages
- Metadata

How we use your information

- To fulfill requests for products, services, Platform functionality, support and information for internal operations
- To customize the content you see when you use the Platform.
- To send promotional materials from us or on behalf of our affiliates and trusted third parties
- To improve and develop our Platform and conduct product development
- To measure and understand the effectiveness of the advertising we serve to you and others and to deliver targeted advertising
- To make suggestions and provide a customized ad experience
- To support the social functions of the Platform
- To use User Content as part of our advertising and marketing campaigns to promote the Platform
- To understand how you use the Platform, including across your devices
- To infer additional information about you, such as your age, gender, and interests
- To help us detect abuse, fraud, and illegal activity on the Platform

- To communicate with you, including to notify you about changes in our services
- To announce you as a winner of our contest, sweepstakes, or promotions if permitted by the promotion rule, and to send you any applicable prizes
- To enforce our terms, conditions, and policies
- Consistent with your permissions, to provide you with location-based services, such as advertising and other personalized content
- For any other purposes disclosed to you at the time we collect your information or pursuant to your consent.

How we share your information

- Service Providers and Business Partners
    - Payment processors and transaction fulfillment providers.
    - Customer and technical support providers.
    - Researchers.
    - Cloud providers.
    - Advertising, marketing, and analytics vendors.
- Within Our Corporate Group
- For Legal Reasons
- With Your Consent

Your Rights

- Request to access or delete the information we have collected about you by sending your request to us at the email or physical address provided in the Contact section at the bottom of this policy.
- To submit a request through an authorized agent.

APPENDIX B – VIGNETTES

Intrusion of solitude

Imagine you are looking at the social media platform whose privacy policy you just read, when you discover an advertisement for a treatment of a condition which you have. Since you have told no one other than your healthcare provider about the condition, you suspect that the social media platform somehow learned about your condition from the healthcare provider and is attempting to use this information to market products to you.

Appropriation of name or likeness

Imagine you are looking at the social media platform whose privacy policy you just read, when you discover a picture of yourself in an advertisement for your healthcare provider. The picture, you notice, was one a friend took and posted to this social media platform several years ago. You never gave your healthcare provider permission to use that image.

Public disclosure of private facts

Imagine you are looking at the social media platform whose privacy policy you just read, when you discover that your diagnosis of an embarrassing medical condition is being shared on social media. Since you have told no one of this diagnosis, you realize that someone from your healthcare provider must have shared it on the social media platform.

False light

Imagine you are looking at the social media platform whose privacy policy you just read, when you discover a picture of yourself in a post by your healthcare provider that suggests you have “Meth Mites,” or sores that some people inflict on themselves as a result of drug induced

hallucinations. These pictures, however, come from your dermatologist who took a before and after photograph (with your permission) of a common skin condition you had.