

Understanding consumer cyber-smearing: a conceptual framework

Haylee Hermann
Kent State University
hhermann@kent.edu

Haithem Zourrig
Kent State University
hzourrig@kent.edu

ABSTRACT

This article proposes a conceptual framework of cyber-smearing, referred here as consumer intentional effort waged to damage the reputation of a business using the Internet as a medium. Drawing upon equity theory (Adams, 1963) and the retributive theory of punishment (Wasserstrom, 1978), we build a conceptual model explaining how betrayed customers may turn into cyber-smearer. A number of cases involving cyber-smearing are discussed. Through this analysis, the key antecedents of cyber-smearing are identified as well. Finally, future research considerations are offered to conclude.

Keywords: Unfairness; Consumer grudge; Retaliation; Cyber-smearing; Business disruption.

1. Introduction

Posting fake negative reviews, referred here as cyber-smearing, could ruin companies' sales and damage their business reputation. Not only, cyber-smearing might hurt businesses but would also disable consumers making an informed decision. Spreading online misinformation about products and services would result in misleading consumers and could unfairly trigger consumer avoidance and boycotting behaviors. With the cloak of anonymity, dishonest consumers could write and share fake negative reviews, which ultimately represent a serious threat to consumers' welfare.

Recent press reports have pointed to the pervasiveness of cyber-smearing worldwide. For instance, in France, a group of restaurant chefs and hotels owners have launched a petition to ban defamatory reviews. They are seemingly irritated to see review sites like TripAdvisor and Yelp enabling anonymous reviewers posting fake and defamatory online reviews. The petition has gathered over 1,700 signatures calling for the end of anonymity of online reviews' posters, more transparency, and accountability, in order to fight against dishonest fake reviews. In the same vein, companies like Google, Amazon, and Facebook have also taken some measures to fight against cyber-smearing and it is not surprising to see these companies responding with litigation; in 2015 Amazon has filed a lawsuit against more than 1,114 individuals who have posted fake reviews on Amazon's website. These fake reviews have significantly undermined the trust that consumers and manufacturers place on Amazon (Bingham, 2015).

Despite being identified as a growing issue, research on consumer cyber-smearing remains limited. Understanding why some customers may turn into cyber-smearer and engage in a campaign waged to damage the credibility and reputation of corporations and businesses could be useful to prevent cyber-smearing and help marketers in directing their efforts to restore corporate reputation.

Drawing upon fairness theory (Adams, 1963) and the retributive theory of punishment (Wasserstrom, 1978), this paper develops a conceptualization of cyber-smearing and proposes a model explaining why and how cyber-smearing occurs. More specifically, service recovery failure, consumer grudge and desire for retaliation are discussed in this paper as key drivers of consumer cyber-smearing, while business disruption is discussed as a direct consequence of cyber-smearing.

The paper is organized in the following fashion: first, we define cyber-smearing and we illustrate this concept with a number of real cases, retrieved from articles and press-papers. Second, building upon fairness theory and retributive theory we propose a conceptual model of cyber-smearing. Then, the antecedents of cyber-smearing (e.g. consumer grudge, desire for retaliation, etc.) and the effect on business disruption are discussed along with propositions development. Finally, we conclude with a discussion about the theoretical and managerial implications as well as further research avenues.

2. Defining Cyber-smearing

Cyber-smearing refers to an intentional effort waged to damage the reputation of an individual or a corporation using the Internet as a medium (Workman, 2012). Examples of cyber-

smearing, include writing untrue negative content on a blog or fake negative reviews on a review site, with the intent to cause harm to individuals or corporation's reputation. Likewise, posting offensive content with personal attacks or content that encourages illegal actions against individuals or a corporation fall under cyber-smearing activities.

Many reports have pointed to the rise of cyber-smearing targeting business. In many instances, small companies have been costly impacted by cyber-smearing, and large corporations as well (Workman, 2012). Cyber-smearing has been also well-documented in press papers and public media reporting many cases of lawsuits alleging cyber defamation and cyber-smearing, several of which have resulted from unhappy customers who have purportedly posted a false and defamatory statement against the corporation or its employees, through tweets, blogs, online reviews, and social media, that could quickly and easily cause widespread damage to a company's reputation. Table 1 provides a sample of cyber-smearing cases.

Table 1: selected cases of cyber-smearing litigation

| <i>Business</i> (Plaintiff) | <i>Cyber-smearer</i> (Defendant) | <i>Litigation case</i> | <i>Court Decision</i> |
|--------------------------------------------|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Loiseau des Ducs Restaurant (France) | Phony reviewer | Posting a fake online review on Yellow pages (i.e. business directory website), a few days before the inauguration of the restaurant. False review, describes the restaurant as “very overrated, it was all show, there was very little on the plate and the only thing that was well loaded was the bill”. | The plaintiff is convicted to a fine of 7,500 for posting a fake online review. Hyperlink: Link 1 |
| Il Giardino Restaurant (France) | Blogger (Caroline Doudet) | Posting a defamatory review on a personal blog . Defamatory review: calling the waitress a “harpy”, the owner “took herself for a diva”, and the restaurant is the one place in town to avoid | The plaintiff is convicted to a fine of €2,500 Hyperlink: Link 2 |
| Hadeed Carpet Cleaning, Inc (USA) | Yelp, Inc | Posting 3 false reviews, written by anonymous on a review website: Yelp | The court ordered Yelp to disclose the identity of anonymous reviewers. Hyperlink: Link 3 |
| Amazon (Worldwide) | 1,114 individuals | In 2015 Amazon filed a lawsuit against more than 1,114 individuals who have posted fake product reviews on Amazon's website . | N/A Hyperlink: Link 4 |
| Nursery (Netherlands) | Google | A nursery in Amsterdam had filed a lawsuit against Google after the latter refused to take down defamatory fake reviews posted on Google reviews and claiming “freedom of speech”. | The court ordered Google to take the false reviews down, pay a compensation to the nursery and disclose the reviewers' identity. Hyperlink: Link 5 |

In many instances, cyber-smearers have been found guilty of posting defamatory and harmful reviews against the company and its employees. For example, in France, a phony reviewer has posted a fake negative review on yellow pages, stating that the restaurant is overrated, there was little on the plate and the only thing that was well loaded was the bill. Ironically the review was posted on yellow pages five days before the inauguration of the restaurant. Noteworthy, since the last few years, there has been a mounting pressure from the court on the review websites to disclose information about the reviewer's identity that victimized business could sue dishonest online reviewer and deter cyber-smearing. For instance, Hadeed Carpet Cleaning, a company from Virginia, had found three anonymous negative reviews criticizing the company, but these did not match with any of their service records.

The business owner has asked Yelp to release the reviewer's information but Yelp refused. Hadeed Carpet Cleaning found at that point that the only option to get this information was to file a case against Yelp for defamation. The court believed that Hadeed Carpet Cleaning had shown enough reasonable evidence that the reviews were, in fact, fake and written by fake customers. Therefore Yelp was forced to disclose the information regarding the reviewers' identity.

While courts are headed in the right direction by ensuring companies are getting treated fairly when it comes to fake online reviews, understanding the motive behind cyber-smearing could help to prevent cyber-smearing and eventually lead to a better outcome than just continually filing multi-million dollar lawsuits. Companies cannot stop cyber-smearing but they can prepare for the inevitable by having damage control mechanisms in place. Prevention and preparation would be certainly the key to combating cyber smears.

3. Theoretical framework

3.1. Cyber-smearing viewed through fairness theory

Fairness theory (Adams, 1963) proposes that individuals who perceive themselves as under-rewarded could experience distress and that this distress leads to efforts to restore equity within a given relationship. Applied to a business-customer relationship context, a customer who perceives his right to getting a fair service and receiving an appropriate service recovery eliminated or threatened, would be motivated to restore fairness. The beliefs that business practices are unjust and that fairness will not be restored would turn a betrayed customer into a cyber-smearer; a self-proclaimed justice doer who undertakes an independent retaliatory action, that is posting a fake negative review to punish the perpetrator firm. In claiming so, the wronged customer becomes a fighter for moral justice.

Assuming there are no other viable options to voice dissatisfaction and that a business may not be receptive to consumer complaints, could be framed by a wronged customer as a goal obstruction (i.e. not getting an appropriate redress following a service recovery failure) and a potential threat to his right of getting a fair service. Hence, the wronged customer becomes motivationally aroused to restore fairness. As all options to get a service recovery are exhausted, taking justice into his own hand becomes the only viable option, which would motivate a customer to engage in a cyber-smearing.

3.2. Cyber-smearing viewed through retributive theory

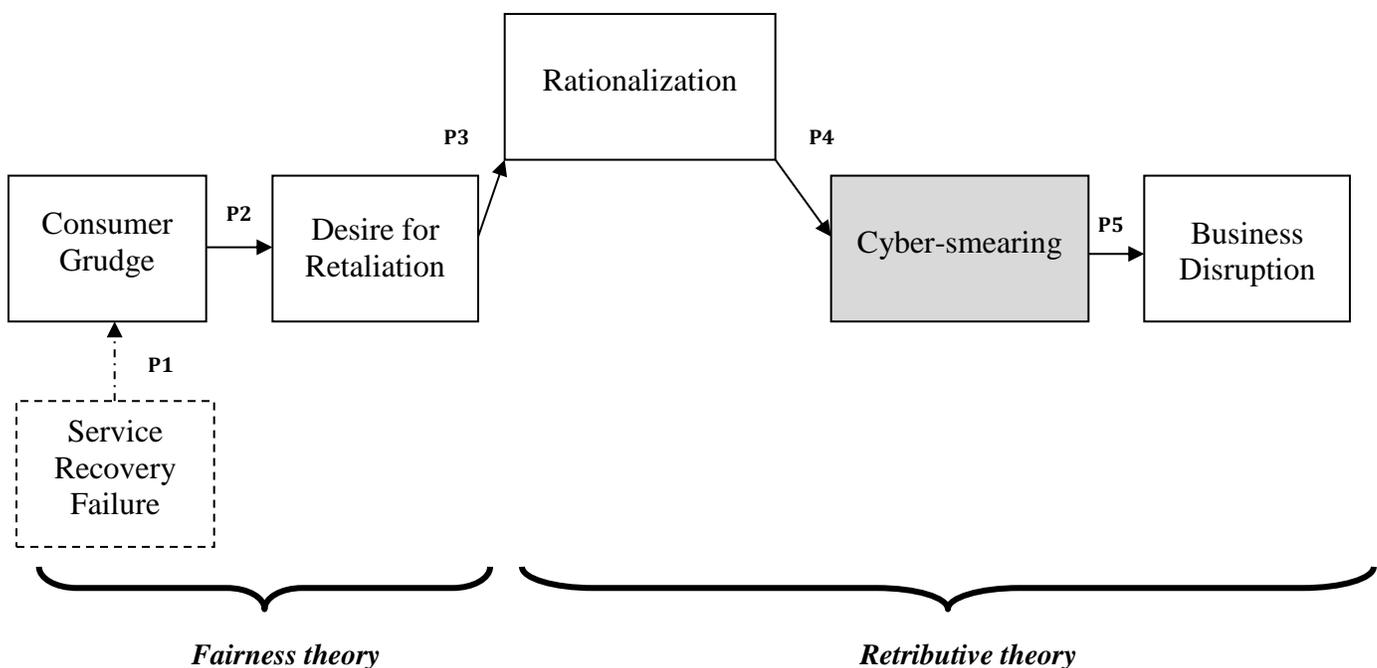
The retributive theory (Wasserstrom, 1978) contends that punishment is a convicted offender's 'just' desert, and relies on the equilibrium between punishment and justice achievement. More explicitly, this theory is based on three main assumptions: first, a person should be punished only if he had voluntarily committed a wrongdoing. Second, the justification for punishing someone is that the return of suffering for moral evil is itself just and morally right. Third, the punishment must match the wickedness of the committed wrong.

Applied to the context of cyber-smearing, the aforementioned assumptions, would provide a clear comprehensive view of the cyber-smearing process. Indeed, before turning into a cyber-smearer, a wronged customer would first blame a business that is believed to be responsible for the service failure and accountable of intentionally undermining any opportunity for redress, which has resulted in a failed service recovery. Further, a wronged customer would justify engaging in cyber-smearing by the need to restore justice, standing up for powerless customers and protecting others from enduring the same sort of injustice.

4. Conceptual Framework

Drawing upon equity theory (Adams, 1963) and retribution justice theory (Wasserstrom, 1978), we develop a cyber-smearing model (see figure 1) that depicts how a consumer could turn into cyber-smearer. The model suggests that a failed service recovery would lead a consumer to hold a grudge against the business which triggers a desire for retaliation. At this stage, the consumer would undergo a rationalization process pertaining to justify potential retaliatory action. The rationalization would trigger cyber-smearing which in turn results in a business disruption.

Figure 1: Model of Cyber-smearing



4.1.Consumer grudge

Consumer grudge refers to a psychological state of maintaining a victim role and experiencing negative emotions associated with some hurtful offense (Bunker & Ball, 2008). Consumers could hold grudge against a business following a service recovery failure (Hunt *et al.*, 1988), but also for other reasons such as the perceived greed, the high exit barriers (Bunker & Ball, 2008), and the belief that a business is neglecting the best interest of society (Nepomuceno *et al.*, 2017). However, the literature review points to the service failure recovery as the main trigger of consumer grudge. If a business is unable to appropriately restore a service after failure, a failed service recovery (i.e. double-deviation situation) would result in a consumer grudge (Bitner *et al.*, 1990). Previous studies have pointed to the vulnerability of failed service recoveries. Unsatisfactory service recovery would have a negative effect on consumer trust (e.g., Holloway *et al.*, 2009). Unsuccessful efforts to recover the initial service failure could threaten and even eliminate customers' right to get an appropriate and fair service recovery. Hence, a failed service recovery could result in consumer grudge. From this P1 flows:

P1. Consumer grudge will be positively related to service failure

4.2.Desire for Retaliation

Holding a grudge has been discussed in the literature as a resentment that is strong enough to justify retaliation (Aron *et al.*, 2006). Consumer grudge could fuel the desire to get even with a business (Grégoire *et al.*, 2009; Joireman *et al.*, 2013).

The feeling of being unfairly treated and the belief that fairness will not be restored may impel some consumers who are grudge holders to bypass conventional ways of voicing dissatisfaction (e.g. formal complaint, negative word of mouth, etc.) and engage in retaliation to punish the business, and achieve revenge and deterrence. From this P2 flows:

P2. Desire for retaliation will be positively related to grudge-holding.

4.3.Rationalization

In fact, when experiencing a strong desire for retaliation, a grudge holder would engage in a rationalization process to self-proclaim a legitimacy of undertaking retaliatory actions against the business, possess a reason and make a legitimate excuse for getting even with the business.

Rationalization involves a cognitive process whereby individuals could justify some behaviours or thoughts that are inconsistent with commonly acceptable conducts and ethical values (Murphy and Dacin, 2011). Rationalization implies a change in one's perception of a situation or a social environment to justify a questionable behavior. Doing so would reduce the underlying negative effect that would normally come with it (Festinger, 1957).

In the context of cyber-smearing, a consumer would post a fake negative review, even he knows the damage that would be done to the business, but still claim the legitimacy of his desire for retaliation. From this P3 flows:

P3. Rationalization will be positively related to the desire for retaliation

4.4.Cyber-smearing

The appraisal of a situation as being unfair to a consumer would increase the desire for retaliation and urge the grudge holder to write and post a fake online review. Cyber-smearing could turn a business' reputation from brilliant to poor. Fake negative online reviews could create the false impression of general customer's dissatisfaction. Existing and potential customers would become influenced by the negativity of the reviews they read. Businesses could work relentlessly to cement their good reputation among their customers. Defamation against the business could undo years of hard work. Thus P4 is offered:

P4.Cyber-smearing will be positively related to the rationalization

4.5.Business disruption

Cyber-smearing activities would result in a loss of revenue, a damage to the business reputation and to an extreme case it would eventually lead to a business disruption that is the interruption of normal business activities (Martin and Kracher 2007).

In many instances, businesses that have been a target of fake online reviews would experience a decline in their sales. This decline is mainly driven by a decrease in customer trust in the business and customer willingness to switch to a competitor having better reviews. Besides, many businesses that fall victim to fake reviews will struggle and find it difficult to acquire new customers in a context of dishonest reviews.

From this P5 flows:

P5. Business disruption will be positively related to cyber-smearing

5. Theoretical and managerial implications

The existence of more intense customer reactions to a service recovery failure such as cyber-smearing remains an intriguing area in need of further theoretical development. The current paper sheds a light on an overlooked online consumer behavior namely cyber-smearing. Albeit conceptual and exploratory in nature, this paper is intended to be the first step for further empirical validation of the developed consumer cyber-smearing model.

While there is very limited empirical research in the applications of fairness theory and retributive theory of punishment to the consumer behavior context, the current paper suggests that both theories would seem relevant to understand the underlying motives of cyber-smearing, and explain how grudge holders turn to social media to seek retribution after a failure of a service recovery. Applied to cyber-smearing, the retributive theory of punishment suggests that cyber-smearing two faces. The first assumes that the inflicted punishment may meet the wickedness of the wrongdoing; and results in restoring fairness and discouraging opportunistic practices of some companies in the market, from this perspective cyber-smearing could be viewed as good and constructive. The second assumes that punishment may exceed the wickedness of the wrongdoing and could be excessive and turns to messy and uncontrollable situations, and often lead to business disruption, in such cyber-smearing could be viewed as ugly.

From a managerial perspective, managers should be aware that if wronged customers voice their dissatisfaction through formal organizational channels (i.e. complaints, etc), and still the failure is not recovered, they risk turning their customers into cyber-smearer, who will the law into their own hands. Understanding what makes consumers turn into cyber-smearing is useful to prevent escalation and to help marketers in directing their efforts to restore their corporate reputation.

Managers should not take for granted that dissatisfied customers might give-up if they don't receive a redress. Recent report converges to the fact that customers now turn to social media to seek retribution after being ignored by companies, as many consumers expressed their willingness to retaliate if their needs are not met. The fact that cyber-smearing may occur in an unpredicted way and unexpected time makes handling conflicting situations with angry customers more difficult, and clearly, customers are becoming less silent than before (Grégoire *et al.*, 2015). Companies cannot eliminate cyber-smearing but at least they could prepare for the inevitable by having damage control mechanisms in place. Prevention and preparing contingency plans are, without a doubt, the key to fight cyber-smearing.

6. Conclusion and further research

The objective of the current research has been to present a conceptual view of the consumer cyber-smearing. Albeit conceptual, this paper identifies some important research avenues that could be pursued to advance this work. For instance, qualitative studies are needed to investigate in-depth customer cyber-smearing phenomenon and to understand the interplay between cyber-cyber-smearing, failed service recovery, and other factors such as perceived low propensity of seeking redress, and customer internet empowerment. In the same vein, developing a scale of cyber-cyber-smearing would be helpful to capture consumers' willingness in engaging in online retaliatory actions. Finally, for the empirical validation of the theoretical model, we argue that a prospective approach such as scenarios represents a reasonable approach to gather data (e.g., Bechwati and Morrin, 2003). Although this approach may limit the external validity of the findings, this method avoids the recall and memory biases as well as biases induced by the way the conflict will be resolved. In addition, using scenarios simulating failed service recovery and borrowed from naturally occurring episodes of real cases of failure may attenuate the lack of the external validity and allow for a control of the content of the experienced service failure across the sample of participants and then supplying standardized stimuli to all subjects, which could enhance the internal validity, measurement reliability and ease of replication (Wason *et al.*, 2002).

References

- Adams, J. S. (1963). Towards an understanding of inequity. *The Journal of Abnormal and Social Psychology*, 67(5), 422.
- Aron, D., Judson, K., Aurand, T. and Gordon, G. (2006), "Consumer Grudgeholding: an ounce of prevention is worth a pound of cure", *Marketing Management Journal*, 16 (1), 158-173.
- Bechwati, N. N., & Morrin, M. (2003). Outraged consumers: Getting even at the expense of getting a good deal. *Journal of Consumer Psychology*, 13(4), 440-453.
- Bingham, J (2015). Users who post 'fake' Amazon reviews could end up in court. The Telegraph, <https://www.telegraph.co.uk/news/shopping-and-consumer-news/11939070/Amazon-sues-more-than-1000-people-over-fake-reviews.html>, last access 07-01-2018.
- Bitner, M. J., Booms, B. H., & Tetreault, M. S. (1990). The service encounter: diagnosing favorable and unfavorable incidents. *The Journal of Marketing*, 71-84.
- Bunker, M. P., & Ball, D. (2008). Causes and consequences of grudge-holding in service relationships. *Journal of Services Marketing*, 22(1), 37-47.
- Festinger, L.: 1957, A Theory of Cognitive Dissonance (Stanford University Press, Stanford, CA).
- Grégoire, Y., Tripp, T. M., & Legoux, R. (2009). When customer love turns into lasting hate: The effects of relationship strength and time on customer revenge and avoidance. *Journal of Marketing*, 73(6), 18-32.
- Grégoire, Y., Salle, A., & Tripp, T. M. (2015). Managing social media crises with your customers: The good, the bad, and the ugly. *Business Horizons*, 58(2), 173-182.
- Holloway, B., Wang, S., & Beatty, S. E. (2009). Betrayal? Relationship quality implications in service recovery. *Journal of Services Marketing*, 23(6), 385-396.
- Joireman, J., Grégoire, Y., Devezer, B., & Tripp, T. M. (2013). When do customers offer firms a "second chance" following a double deviation? The impact of inferred firm motives on customer revenge and reconciliation. *Journal of Retailing*, 89(3), 315-337.
- Martin, K. D., & Kracher, B. (2007). A conceptual framework for online business protest tactics and criteria for their effectiveness. *Business & Society*, 47(3), 291-311.
- Murphy, P. R., & Dacin, M. T. (2011). Psychological pathways to fraud: Understanding and preventing fraud in organizations. *Journal of Business Ethics*, 101(4), 601-618.

Nepomuceno, M. V., Rohani, M., & Grégoire, Y. (2017). Consumer resistance: From anti-consumption to revenge. *In Consumer Perception of Product Risks and Benefits* (pp. 345-364). Springer, Cham.

Wason, K. D., Polonsky, M. J., & Hyman, M. R. (2002). Designing vignette studies in marketing. *Australasian Marketing Journal (AMJ)*, 10(3), 41-58.

Wasserstrom (1978), "Retribution and the Theory of Punishment," *Journal of Philosophy*, 75, 601-20.

Workman, M. (2012). Rash impulsivity, vengefulness, virtual-self and amplification of ethical relativism on cyber-smearing against corporations. *Computers in Human Behavior*, 28(1), 217-225.