A Perfect Fit: Personalization Versus Privacy

Joni R. Jackson
Chicago State University

Certain marketing tactics make people feel "creepy" because they are invasive and may violate social norms. People's concerns about how their personal data is collected and used may be heightened as companies' ability to collect and use personal data increases. One way to allay people's concerns is to build a relationship, a friendship that might moderate concerns about intrusive tactics. Two hundred twenty-three participants evaluated three vignettes describing scenarios where marketers collect and share personal data. Participants felt most creepy when brands collected and shared personal data publicly. Having a relationship (brand friend) may moderate feelings of creepiness.

INTRODUCTION

Customization is "at the heart of relationship marketing," and improvements in technology allow companies to gather massive amounts of data that allow them to deliver "perfectly personalized experiences" (Coll, 2013; Falcon & Hamamoto, 2017). Personalized customization is one way for companies to befriend consumers. However, there is a need to balance personalization with privacy.

Concerns about the sharing and use of personal data are heightened among consumers as companies' ability to collect and use personal data increases (Rainie & Duggan, 2016; TRUSTe Privacy Index 2016). Some activities related to the collection and use of personal data may be perceived by consumers as harmless or relatively benign; however, other activities may be perceived as violations of accepted social norms. Target, the big-box discount retailer, left some of its consumers feeling somewhat "creepy" when it used an algorithm to determine if a woman was pregnant (Duhigg, 2012). Target used this information to customize promotions and develop targeted behavioral ads. More recently, Cambridge Analytica accessed Facebook user data - people's identities, friend networks, and "likes" - to customize their news feeds (Granville, 2018). These types of tactics may feel invasive, leaving people uncomfortable or feeling "creepy." Moreover, these types of tactics might damage a company's relationship with its consumers (Moore, Moore, Shanahan, Horky, & Mack, 2015), particularly if these tactics give rise to privacy violations.

PRIVACY AND TRUST

Definitions of privacy are varied and include the notion of information that is inaccessible (Warren & Brandeis, 1890) and information that is controlled (Westin, 1967). Nissenbaum (2004) suggested that privacy is defined by context (i.e., person, situation, and relationship). van den Hoven (2008) described privacy as a "fuzzy" concept, a definition that stems, in part, from the contextual nature of privacy, one based on social norms that dictate what is a public space or a private space as well as the appropriate norms that operate within that space (Nissenbaum, 2004; Solove, 2006; Moor, 1997).

Improvements in technology - advanced data mining techniques, ubiquitous smart phone cameras - increase our ability to capture data (Solove, 2006) and add to our challenge in defining context - what constitutes a public versus a private space (Tene & Polonsky, 2013; Marx, 2016). Information that is appropriate to access and share is determined by context and how we define that context.

A recent incident highlights the challenges privacy scholars face in defining what constitutes privacy and private spaces. In 2018 an Uber and Lyft driver recorded and secretly live-streamed his passengers on Twitch, a website now owned by Amazon, which was a place to watch people playing video games live. Although many described the driver's actions as "creepy," he did not violate his state's law by recording and live-streaming his passengers, who may or may not have had a "reasonable expectation of privacy" (Heffernan, 2018; Zavari, 2018). He may, however, have violated social norms that govern behavior in a ride share situation, although even that is not clear because these norms are evolving. Clearly, the driver defined the space his passengers occupied in his vehicle as public; yet, in an ironic twist, the driver requested that his name not be disclosed, in order to "protect his privacy." This situation illustrates the fuzzy nature of privacy and the lack of clarity given shifting social norms that help us define context and determine what information can be gathered and by whom.

One way to allay people's privacy concerns is to build a relationship that may foster perceptions of trust and honesty. An important factor in consumers' perceptions of trust and honesty is the understanding of how their personal data or information is shared with or used by others (Culnan & Bies, 2003; Solove, 2006). It is here where we see the greatest threat and the greatest potential from the use of an individual's data.

Consumers are willing to share private information, often in exchange for some benefit, such as personalized customization (Beales & Muris, 2008). When consumers agree to participate in an exchange, there may be an implied agreement (Culnan and Bies 2003) regarding how companies use their data and their expectations of privacy. The idea of an implied agreement can create a context for trust, and consumers appear less concerned about data collected by companies or brands they trust because this relationship implies less potential for abuse of personal information (Martin, 2018). Key drivers of trust are experience with a company and a relationship with a brand (Beitelspacher, Hansen, Johnston, & Deitz, 2012; Culnan & Armstrong, 1999; Jackson; 2016; Milne & Boza, 1999; Milne, Rohm & Bahl, 2008; Milne, Pettinico, Hajjat, & Markos, 2017). However, Madden (2017) found that many people do not have confidence in institutions that handle their personal data, and many fear that they have lost control of their personal data (Olmstead & Smith, 2017). If consumers cannot control their data, or if the process of collection and use is not transparent, trust in the company or brand may decrease (Newman, 2014).

Consumers' relationships with brands can often resemble their relationships with people. Just as there are norms that dictate the rules of a relationship among people, similar rules exist when people think of brands as best friends (MacInnis & Folkes, 2017). Belanger, Hiller, and Smith (2002) found that people's willingness to share personal information was based on perceptions of a company's trustworthiness (e.g., Amazon). Positive experience with a brand is a factor in building brand trust. Trust, in turn, sets people's expectations for the norms that should operate in a relationship with the trusted brand (Xingyuan, Li, & Wei, 2010) - like one's relationship with a best friend - and define the parameters for balancing privacy with personalization (Culnan & Bies, 2003).

People's willingness to share information also stems from having some control or say in how their personal data is collected and used. However, given advances in technology and more sophisticated options for data collection and aggregation, increasingly data collection occurs without consumer voice or control. This loss of control may raise consumer concerns about how their personal data and information will be used and shared. Yet it is through the use of consumers' data that companies come to know people as well as they do (similar to a relationship with a friend). Developments in technology as well as more sophisticated data gathering and marketing analytic techniques increase the volume of data that marketers can use to customize and personalize consumer offerings and experiences.

In this paper, we explore people's relationships with their favorite brand by examining their reactions to three vignettes that describe hypothetical scenarios in which their favorite brands collect and use their personal data. We manipulate context - private versus public - by varying how one's hypothetical data is collected (provided by the participant through a survey or collected by the favorite brand without the participant's input). Privacy is manipulated by hypothetical access to one's profile (access limited to the participant or widely available to the public). Further, we explore the extent to which concerns about privacy, feelings about companies sharing personal data, and beliefs about brands as best friends affect how comfortable or creepy people feel about a brand's collection and use of their personal data.

METHOD

Invitations to participate in this study were sent via email, text messaging, and Facebook. Participants were asked to forward the invitation to friends and associates (snowballing). The sample was a convenience sample. All participants volunteered; no one received payment for participation. Some college students may have received course credit from their professors. Two hundred and twenty-three people participated in the study.

Participants were sent a link to an anonymous survey, which was administered online using Survey Monkey. Internet Protocol (IP) addresses and other identifying information were not collected. The short survey took 5-10 minutes to complete and asked participants to answer questions about the three vignettes; questions related to privacy concerns, information sharing and brands as best friends; and, five questions about demographics.

For the vignettes, people were asked to imagine their favorite brand while reading each of the three vignettes. The vignettes described various scenarios in which the favorite brand collected their personal information. After each scenario, participants were asked to rate how comfortable or creepy they felt about their favorite brand collecting and using their personal data.

All three vignettes stated the following: "Imagine your favorite brand creates a profile of your lifestyle, personality, and shopping habits. Your brand knows you really well because your profile describes you just like a best friend would. Please move the sliding scales to rate how creepy (-5) or comfortable (+5) you feel." The differences among the three vignettes were as follows.

- Vignette 1: Your profile is based on your answers to a survey. Only you and your favorite brand can see your profile.
- Vignette 2: Your profile is based on information your brand collected about you. Only you and your favorite brand can see your profile.
- Vignette 3: Your profile is based on information your brand collected about you. Anyone can see your profile.

Following the three vignettes, participants were asked three questions:

1. I am not concerned about my privacy because I have nothing to hide.
2. It is okay for a company to share my personal information.
3. My favorite brand is like my best friend.

Finally, participants were asked demographic questions about their age, gender, ethnicity, highest level of education, and household income.

We predicted that people would be most concerned about a brand's use of their personal data when that data was collected without their permission and when that information was made public. Thus, we predicted that people were more likely to report feeling "creepy" in Vignette 3, the scenario in which their data is collected by the brand and then made public. We predicted that if people were not concerned about privacy, their responses to the three vignettes would not differ.

If a favorite brand is like a best friend, we predicted that this would moderate people's concerns about a brand's use of their personal data. Thus, we expected that when a favorite brand is like a best friend, the brand's collection and use of people's personal data would be less likely to trigger feelings of discomfort (or feeling creepy).

Finally, we explored differences that might emerge based on demographics. Ethnic minority groups and people with lower incomes have reported greater concerns about the collection and use of their personal data (Madden, 2017); members of these populations might be more concerned about being the target of profiling.

FINDINGS

The Sample

Our sample was fairly diverse. Slightly over forty percent of the sample was traditional college age students (18-24 years of age); about one-third was between 25 - 54 years of age; and, almost twenty percent were over 55 years of age. Over sixty percent of the sample (64.1%) was female. Forty percent of participants identified as Black/African American (40.4%), while over thirty percent identified as White/European American (37.2%). The remaining participants identified as LatinX (4%), multi-racial (4.5%), or Asian (2.7%). About 10% of participants declined to indicate ethnicity; one participant indicated “other,” one indicated “Jewish,” and one indicated “American Indian.”

Over half of White/European American participants (53%) had completed high school or a GED. Among Black/African American participants, almost 60% had completed college (holding a bachelors, masters, professional or doctoral degree). About thirty percent of participants reported household incomes below $49K (30.5%); almost thirty percent of participants reported household incomes between $49K - $99K (28.7%); and, twenty-five percent of participants reported household incomes over $100K (the remaining did not report).

The Vignettes - Privacy Scenarios

We predicted that people would report more concern (or feel creepy) about a brand’s use of their personal data when that data was collected without their permission (e.g., brand profiles created in Vignettes 2 and 3) and when that private data was made public (Vignette 3). Participants indicated the extent to which the scenarios described in the vignettes made them “feel creepy” (-5) or comfortable (+5) (See Table 1).

TABLE 1

VIGNETTES	ALL PARTICIPANTS MEAN RESPONSE*
Vignette 1: Survey-Private (n = 214)	1.96
Vignette 2: Brand Created Profile-Private (n = 210)	1.46
Vignette 3: Brand Created Profile - Public (n = 207)	-1.67
ADDITIONAL QUESTIONS	**ALL PARTICIPANTS MEAN RESPONSE***
Not Concerned About Privacy (n = 207)	-1.48
Okay to Share Personal Information (n = 207)	-3.76
A Favorite Brand is Like A Best Friend (n = 206)	-1.04

*Higher means indicate that participants were more comfortable with the scenario or agreed with the statement; lower means indicate that participants felt more “creepy” or disagreed with the statement.

As predicted, participants were less comfortable with Vignette 3 (mean = -1.67), the scenario in which the brand created a profile based on information the company collected and then made public.

Moreover, our findings suggest that people were concerned about their privacy (mean = -1.48) and concerned about their personal information being shared by a brand (mean = -3.67). Participants tended to disagree with the statement, a brand is like a best friend (mean = -1.04), although younger people (those under 34 years of age) were more likely to think of a brand as a best friend than people who were older (those 35 years of age and older).

We were also interested in the extent to which concern about privacy, sharing personal information, and perceptions of brand as a best friend predicted participants' responses to the three vignettes. The mean scores for the three vignettes and the questions regarding concern about privacy, sharing personal information, and perceptions of a brand as a best friend were converted to z-scores. A linear regression was conducted using z-scores.

Concern about privacy was a significant predictor of participants' responses to all three vignettes. While the results were significant for all three vignettes, concern about privacy explained 24.3% of the variance in responses to Vignette 3, the scenario in which people's information is collected by the brand and made public. Concern about a brand sharing personal information was also a significant predictor of participants' responses to all three vignettes; concern about a brand sharing personal information explained 20.9% of the variance in responses to Vignette 3. Finally, perception of a brand as a best friend was a predictor of responses to all three vignettes; being best friends with a brand appears to moderate people's concerns about the collection and use of their data (See Table 2).

TABLE 2

	Concern about Privacy F (1, 205)	**R^2**	**Sharing Personal Information F (1, 205)**	**R^2**	**Brand as Best Friend F (1, 204)**	**R^2**
Vignette 1	13.633**	0.062	7.624*	0.034	21.802**	0.097
Vignette 2	26.691**	0.115	12.193*	0.056	34.665**	0.145
Vignette 3	65.702**	**0.243**	54.306**	**0.209**	26.033**	0.113

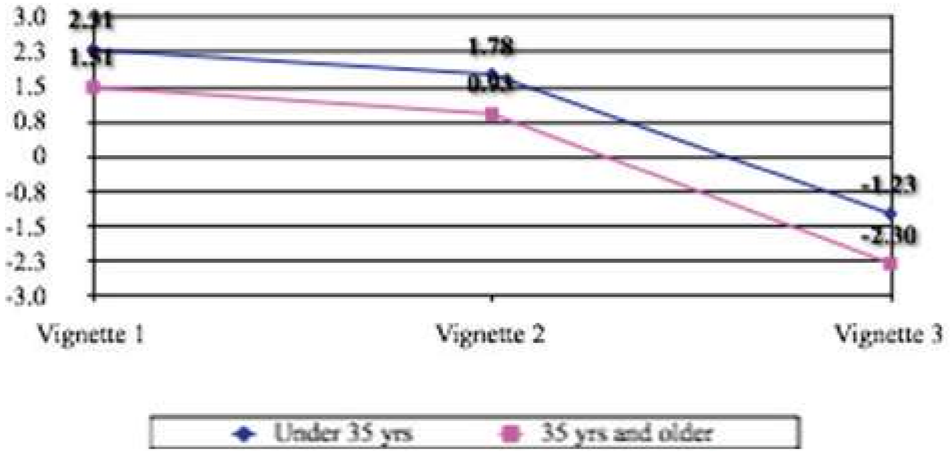
* p < .008; ** p = .000

Demographics

We also sought to examine the impact of demographics - age, education and income on participants' responses to the three vignettes (there were no differences based on ethnicity).

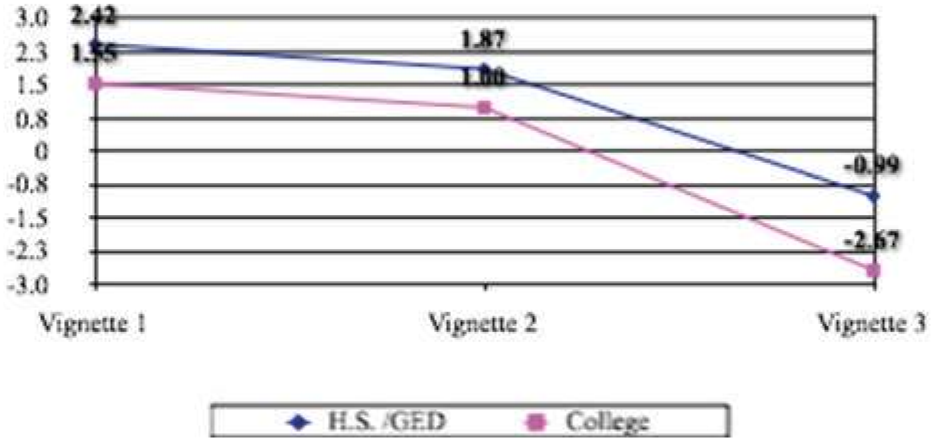
First, we examined age. A preliminary analysis had uncovered differences between younger and older participants. Therefore, we created two new age categories, participants under 35 years of age (i.e., those 18 - 34) and participants 35 years and older. While both groups indicated that they felt more creepy (or less comfortable) with Vignette 3, people 35 years and older were more likely than people under 35 years old to indicate that they felt creepy when brands gathered their data and made that data public (Vignette 3). All differences were significant (p < .05) (See Figure 1).

FIGURE1
VIGNETTE MEAN RESPONSE BY AGE



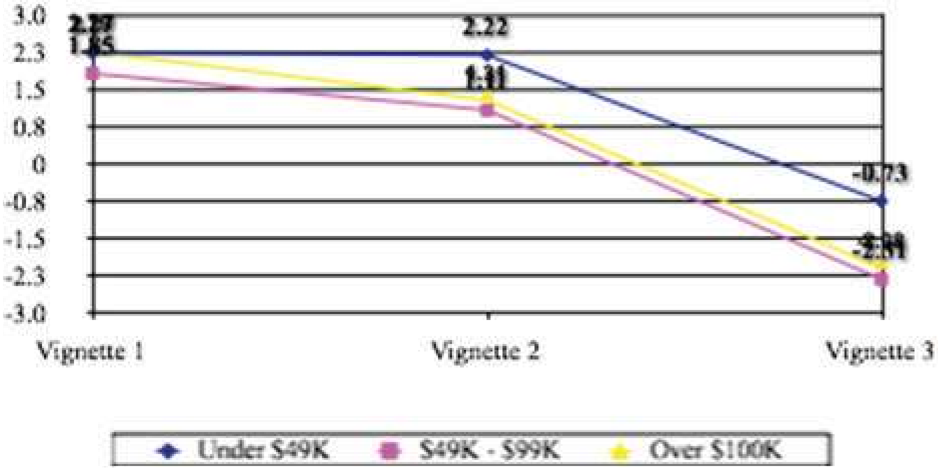
Next, we examined education. We created two new categories, high school (GED) graduates and college graduates. While both groups indicated that they felt more creepy (or less comfortable) with Vignette 3, people whose highest level of education was college were more likely than people whose highest level of education was high school to indicate that they felt creepy when brands gathered their data and made that data public (Vignette 3). All differences were significant (p < .05) (See Figure 2).

FIGURE 2
VIGNETTE MEAN RESPONSE BY EDUCATION



Finally, we examined household income. While all household income groups indicated that they felt more creepy with Vignette 3, people with higher household incomes (over $49K) were more likely to indicate that Vignettes 2 and 3 made them feel creepy than people with lower household incomes. This effect was more pronounced for Vignette 3 than Vignette 2. The differences between those with household incomes of $49K or more and those with household income below $49K were significant (p < .05) for Vignettes 2 and 3 (See Figure 3).

FIGURE 3
VIGNETTE MEAN RESPONSE BY INCOME



DISCUSSION

We predicted that people would be most concerned about a brand's use of their personal data when that data was collected without their permission and when that information was made public. Participants reported feeling more "creepy" with Vignette 3, where their (hypothetical) data was collected by the brand and then made public. Vignette 2, where people's (hypothetical) data was collected by the brand but kept private, made people feel less comfortable, but not to the extent that the public release of data did (Vignette 3). And finally, the scenario that made people feel the least uncomfortable was Vignette 1, the scenario where participants provided their (hypothetical) data to the brand, which then kept that data private (One scenario was missing from our design - the version of Vignette 1 where data was made public. The exclusion of this scenario (unintentionally) did not allow us to examine the main effect of making data public.)

We also sought to examine the role of a favorite brand as a best friend; we predicted that thinking of one's favorite brand would moderate people's concerns about a brand's use of their personal data. While this seemed to be the case, we are cautious with regard to any conclusions about the impact of our brand-as-best-friend manipulation. We did not include a check of this manipulation, and thus are not able to determine how effective this manipulation was (i.e., we do not know what people imagined when they thought of "favorite brand").

Marketers have to be cautious in their efforts to build trust, intimacy or friendships with consumers. Some researchers have cautioned that marketers' efforts to develop long-term relationships or friendships with consumers by developing intimacy, might be perceived as intrusive or creepy (Moore et al., 2015; O'Malley, L., M. Patterson & M. Evans, 1997). When we think of friendships, we often think of someone whom we trust. Favorite brands are favorites because they share people's values and are trusted, like best friends (Jackson, 2016). Indeed, favorite brands have been found to evoke emotional responses similar to that of interpersonal friendships (Langner, Schmidt, & Fischer, 2015). Thus, when people see a brand as a best friend, concern about the use of their personal data may be mitigated by the belief that a brand, like a best friend, will not use personal information in a manner likely to cause harm.

It seems clear, from our data, however that people did not think that it is okay for a brand to share their personal information. Our sample voiced strong feelings regarding this statement. Their responses may reflect growing knowledge among consumers about the vast amounts of data that are captured and used in ways that are beyond their control. As Gandy noted, there are "consequential decisions being made without our knowledge and consent that affect our privacy as well as our autonomy" (Gandy, 2018).

Whether or not participants are aware, their responses may reflect some sense of how their data is being used. Today, many companies combine people's data and infer things that might otherwise have remained private ("the mosaic effect"); these inferences can be used to manipulate people's behavior (Gandy, 2017; Wedel & Kannan, 2016).

In March 2018, news broke about Facebook's involvement in the release of information about 50 million of its users (the Cambridge Analytica case which sought to manipulate voter behavior); Facebook saw its market capitalization drop $70B in 10 days. There were a number of factors that may have lead to the drop in market capitalization, one of which was trust in Facebook (or its CEO Mark Zuckerberg). "Opinion polls in the United States, Canada and Germany cast doubt over the trust people have in Facebook… fewer than half of Americans trust Facebook to obey U.S. privacy laws … 60 percent of Germans fear that Facebook is having a negative impact on democracy" (Reuters, 2018). When trust in the brand dropped, its stock suffered a precipitous decline. Whether this effect is long-term remains to be seen.

However, this example, along with the earlier Target and Uber/Lyft examples, point to the challenge for marketers. Whether people experience comfort or creepiness is posited to be a function of context and whether that context is defined as public or private. Context is important because it dictates the norms that operate when a brand uses people's personal information (Nissenbaum, 2004; Solove, 2006). Creepiness emerges when actions "push against traditional social norms" or occur in contexts where social norms are still evolving" (Tene & Polonetsky, 2013). Improvements in technology drive many of the changes in the definition of context and norms. While technology makes it easier to collect data and track and monitor people, newly emergent technology does not come with a set of rules that define the appropriate collection and use of data (Falcon & Hamamoto, 2017). Arguably, much of the tracking and monitoring may be benign, however it can make one feel creepy, even if there is not harm. When marketers create profiles of their customers in order to personalize and customize their offerings, they may make people feel creepy because they know far too much about people (Moore, Moore, Shanahan, Horky, & Mack, 2015). Trusted brands should exercise caution as they push to personalize their offerings.

REFERENCES

Beales, J.H., & Muris, T. J. (2008). Choice or consequences: Protecting privacy in commercial information. *The University of Chicago Law Review*, 75(1), 109-135. Retrieved from http://www.jstor.org/stable/20141902.

Beitelspacher, L. S., Hansen, J. D., Johnston, A. C., & Deitz, G. D. (2012). Exploring consumer privacy concerns and RFID technology: The impact of fear appeals on consumer behaviors. *Journal of Marketing Theory & Practice*, 20(2), 147-160.

Belanger, F., Hiller, J.S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, 11(3-4), 245 - 270. https://doi.org/10.1016/S0963-8687(02)00018-5.

Coll, S. (2013). Consumption as biopower: Governing bodies with loyalty cards. *Journal of Consumer Culture*, 13(3), 201 - 220. https://doi-org.proxy.uchicago.edu/10.1177/1469540513480159.

Culnan, M. J., & Armstrong, P.K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104-115. Retrieved from http://www.jstor.org/stable/2640390.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, 59(2), 323-342.

Duhigg, D. (2012). *How companies learn your secrets*. *The New York Times Magazine*. Retrieved from https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

Falcon, R., & Hamamoto, B. (2017). Bodies of data. Who are we through the eyes of algorithms? *Future Now*. Retrieved from http://www.iftf.org/future-now/article-detail/bodies-of-data/.

Gandy, O.H. (2017). Surveillance and the formation of public policy. *Surveillance & Society*, 15(1), 158-171. Retrieved from http://library.queensu.ca/ojs/index.php/surveillance-and-society/index.

Granville, K. (2018). *Facebook and Cambridge Analytica: What you need to know as fallout widens*. *The New York Times*. Retrieved from https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

Heffernan, E. (2018). *St. Louis Uber driver has put video of hundreds of passengers online. Most have no idea*. *St. Louis Post Dispatch*. Retrieved from https://www.stltoday.com/news/local/metro/st-louis-uber-driver-has-put-video-of-hundreds-of/article_9060fd2f-f683-5321-8c67-ebba5559c753.html.

Jackson, J.R. (2016). Big data: Goldmine or minefield? *American Journal of Management*, 16(4), 57 - 64.

Langner, T., Schmidt, J., & Fischer, A. (2015). Is it really love? A comparative investigation of the emotional nature of brand and interpersonal love. *Psychology & Marketing*, 32(6), 624 - 634. doi:10.1002/mar.20805.

MacInnis, D. J., & Folkes, V. S. (2017). Humanizing brands: When brands seem to be like me, part of me, and in a relationship with me. *Journal of Consumer Psychology*, 27(3), 355 - 374. https://doi.org/10.1016/j.jcps.2016.12.003.

Madden, M. (2017). *Privacy, security and digital inequality: How technology experiences and resources vary by socioeconomic status, race, and ethnicity*. *Data & Society Research Institute*.

Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Ethics*, 82, 103-116.

Marx, G. T. (2016). *Windows Into the Soul: Surveillance and Society in an Age of High Technology*. Chicago: University of Chicago Press.

Milne, G. R., Bahl, S., & Rohm, A. (2008) Toward a framework for assessing covert marketing practices. *Journal of Public Policy & Marketing*, 27(1), 57-62.

Milne, G. R., & Boza, M. (1999). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing*, 13(1), 5-24.

Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2017). Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing. *Journal of Consumer Affairs*, 51(1), 133-161.

Moor, J. H. (1997). Towards a Theory of Privacy in the Information Age. *Computers and Society*, 3, 27.

Moore, R.S., Moore, M.L., Shanahan, K.J., Horky, A., & Mack, B. (2015). Creepy marketing: Three dimensions of perceived excessive online privacy violation. *Marketing Management Journal*, 25(1), 42-53.

Newman, N. (2104). How big data enables economic harm to consumers, especially to low-income and other vulnerable sectors of the population. *Journal of Internet Law*, 18(6), 11-23.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 119 - 158.

Olmstead, K., & Smith, A. (2017). *Americans and cybersecurity*. *Pew Research Center: Internet & Technology*. Retrieved from http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

O'Malley, L., Patterson, M., & Evans, M. (1997). Intimacy or intrusion? The privacy dilemma for relationship marketing in consumer markets. *Journal of Marketing Management*, 13(6), 541 - 559.

Rainie, L. & Duggan, M. (2016). *Privacy and information sharing*. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.

Reuters. (2018). *Facebook has lost $70 billion in 10 days — and now advertisers are pulling out*. *Financial Post*. Retrieved from https://business.financialpost.com/technology/u-s-ftc-investigating-facebooks-privacy-practices.

Solove, D. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), 477-564. doi:10.2307/40041279.

Tene, O., & Polonetsky, J. (2013). A theory of creepy: Technology, privacy and shifting social norms. *Yale Journal of Law and Technology*, 16 or 59, 59-102.

TRUSTe. (2016). *TRUSTe/National Cyber-Security Alliance: U.S. consumer privacy index*. San Francisco. Retrieved from https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-us/.

Warren, S.D., & Brandeis, L.D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193 - 220. doi:10.2307/1321160.

Tsui, L. (2018). *Lokman Tsui (Ph.D. '10) Interviews Oscar Gandy on personal data protection, privacy, and surveillance*. *The Annenberg School for Communications at the University of Pennslyvania*. Retrieved from https://www.asc.upenn.edu/news-events/news/personal-data-protection-privacy-and-surveillance.

van den Hoven, J. (2008a). Information Technology, Privacy, and the Protection of Personal Data. In J. van den Hoven & J. Weckert (Eds.), *Information Technology and Moral Philosophy*, (pp. 301-321). Cambridge: Cambridge University Press.

Wedel, M., & Kannan, P. K. (2016). Marketing analytics for data-rich environments. *Journal of Marketing*, 80(6), 97 - 121. doi:10.1509/jm.15.0413.

Westin, A. F. (1967). *Privacy and Freedom. Alan F. Westin; foreword by Oscar M. Ruebhausen*. New York: Atheneum.

Xingyuan, W., Li, F., & Wei, Y. (2010). Development and validation of a brand trust scale. *International Journal of Market Research*, 45(1), 35 – 53.

Zaveri, M. (2018). *St. Louis Uber and Lyft driver secretly live-streamed passengers, report says*. *The New York Times*. Retrieved from https://www.nytimes.com/2018/07/22/technology/uber-lyft-driver-live-stream-passengers-nyt.html.