Privacy, Trust, and Manipulation in Online Relationships

Esma Aïmeur and Zakaria Sahnoune

University of Montreal, Montreal, Quebec, Canada

ABSTRACT
This work studies factors that influence personal information disclosure coming from vulnerable users who may adopt risky online behavior on social media. These users trust their online relationships and reveal confidential or sensitive information, causing damage to themselves and their relatives and friends. We carried a survey-based study on 1,532 participants to see if they would reveal sensitive information when they have close online relationships whom they trust. The results led to several discoveries, especially concerning the factors affecting the disclosure in online relationships, and those affecting the attitude toward online manipulation. Moreover, this study attested a strong positive relation between disclosure issues and the user’s attitudes toward manipulation. The latter which is affected by their online behavior and social interaction ties. In a nutshell, users attitudes toward manipulation may lead to self-disclosure on the one hand, and these attitudes could be identified through their social behavior on the other hand.

ARTICLE HISTORY
Received 4 January 2018
Accepted 16 April 2019

KEYWORDS
Computer-mediated communication; confidentiality and privacy of information; social networking; Internet driven manipulation; information disclosure

Introduction
In the age of exposure, privacy is an important issue. Westin (Westin, 1968) defines privacy by four functions. Personal autonomy that allows us to be free from manipulation by others and thus offers more control over our own lives and outcomes. Emotional release from the demands of impression management and emotion regulation that goes along with living within a social group. Self-evaluation, providing a space to process and evaluate experiences and find meaning in them. Limited and protected communication that both sets boundaries and, for people within our boundaries, can help. Moreover, and along with the previous privacy requirements, the problem of control over personal data has become inextricably linked to personal choice, autonomy, and socioeconomic power (Acquisti, Brandimarte, & Loewenstein, 2015).

Social media are widely used nowadays and the privacy breaches related to misusing them constitute a potential risk vector for individuals that are
concerned about their information being disclosed. Similarly, the way information is organized and exchanged in social media may help in revealing sensitive information (Aïmeur, Brassard, & Rioux, 2013), which was much harder two decades ago.

As stated by Coons (Coons & Weber, 2014):

> We are social creatures, and as such, we influence one another in a variety of ways … Manipulation is understated but has perhaps the more pervasive type of impact. Manipulation manifests itself in many aspects of life: advertising, politics, and in both professional and intimate relations.

Therefore, the manipulation in this work refers to the action of using deceptive manners to make someone do something while revealing other intentions.

Social media users’ information is protected by their credentials, and manipulators are more likely to target those credentials to gain full access to the personal data of their victims. In this context, the word “credentials” describes the information used by social media users to access their account (i.e., e-mail address, phone number, username, and password). In some cases, the credentials could be disclosed by giving access to a device (e.g., giving his/her smartphone to another person). However, this latter needs physical meetings, which is not the context of this work. Compared to public self-disclosure on social media, which refers to disclosing information to a group of users (e.g., post on Facebook or Twitter), the damage of self-disclosure in one-on-one communications is more dangerous. The information disclosed is usually more sensitive, which implies risks of heavier costs such as: cyberbullying, reputation damage, identity theft, and others. Indeed, the damage could be worse if the manipulator is a deceiver (Tsikerdekis & Zeadally, 2014).

This article presents a survey-based study that investigates sensitive data disclosure issues related to online manipulation. It draws away from public self-disclosure, which does not include the disclosure of credentials, while it focuses on the impact of manipulation among other factors affecting self-disclosure in one-on-one relationships.

To explain our motivations, we consider a fictitious scenario that describes a self-disclosure case. It summarizes the personal effects of manipulation in e-relationships.

The use-case scenario is such that two people, Alice and Chuck, living in different countries meet on vacation. Once back, Chuck initiates an online relationship (called e-relationship) through social media with Alice. When the e-relationship begins to be more intimate, Chuck becomes more controlling and, therefore, starts to manipulate his e-partner Alice to get her online credentials (e.g., accounts, passwords). The latter may lead to mind control, blackmail, and mental abuse, changing the so-called excellent relationship to a toxic one. Alice might be depressed and may not recover.
While fictitious, the above scenario represents a specific case of manipulation caused by *online deception* (Tsikerdekis & Zeadally, 2014). In a nutshell, while online deception deals with the general case of lying and misleading other users online (Ebner et al., 2018; Singh, Sharma, Thakral, & Choudhury, 2018; Van der Walt, Eloff, & Grobler, 2018), manipulation, this article deals with the specific case where a manipulator uses deception methods to manipulate a victim and potentially gets access to his/her personal data.

This work is based on *online social psychology*, and more precisely, we are interested in studying Communication Privacy Management (CPM) Theory (Petronio, 2012). This theory extended Altman’s work (Altman & Taylor, 1973; Taylor & Altman, 1966; Taylor, Altman, & Sorrentino, 1969) on privacy management and sought to answer the following questions: how do people decide when and what to disclose, how do they prevent unwanted disclosure, and how do they deal with unwanted disclosure when it occurs? As stated in (Zurbriggen, Ben Hagai, & Leon, 2016) CPM includes five principles, namely:

1. *Privacy ownership*, People believe that their private information belongs to them.
2. *Privacy control*, only they should have the right to control access to it.
3. To *protect control* of their information, people develop and use *privacy rules* to decide whether and when to reveal or conceal personal information.
4. *Co-ownership*, explicitly acknowledges that, whenever information is shared, protection of that information must henceforth be coordinated with the other people who now possess that information.
5. *Privacy turbulence*, which occurs if unauthorized others gain access to one’s personal information, either accidentally or through the deliberate actions of a co-owner.

We adapted the JSDK Jourard’s questionnaire (Jourard & Lasakow, 1958) and the Taylor and colleagues’ categorization (Altman & Taylor, 1973; Taylor et al., 1969, 1969) and applied them to the digital age. This article is organized as follows. In the second section we explore the state of the art through a literature review, and then we present our research model in the third section. The fourth and fifth sections focus on data collection, testing, and analysis followed by a discussion of the results. The latter is followed by a conclusion and potential future directions for research.

**Theoretical background**

In social psychology, self-disclosure was defined by Jourard (Jourard & Lasakow, 1958) as “Any information about himself which person A
communicates verbally to a person B.” Moreover, self-disclosing behavior may be seen as a product of two opposing forces, one operating to increase disclosure, the other operating to inhibit it (Cozby, 1973).

Today, social media pose a privacy paradox (Barnes, 2006); most users indicate that they are concerned about their privacy, yet they disclose themselves and share personal information on social media platforms. In any case, some technology leaders think that privacy is lost and sharing personal information is now the norm (Bradbury, 2015). However, social science research suggests that privacy is essential for human functions such as autonomy, development, and creativity (Livingstone, 2008). Stein and Sinha refer to privacy as “the rights of individuals to enjoy autonomy, to be left alone, and to determine whether and how information about one’s self is revealed to others” (Stein & Sinha, 2002, p. 414).

Similarly, an online environment that ensures privacy may promote constructive self-expression, sociability, and community engagement which participate in forging one’s positive development and creativity (Livingstone, 2008).

Sharing confidential information and disclosing intimate information about oneself usually only occurs after trust has been established between partners. In the digital world, premature disclosure occurs much easier and faster. Disclosure may include thoughts, feelings, goals, fears, dreams, embarrassments, likes, dislikes, and successes and failures (Aïmeur et al., 2013; Aïmeur, Brassard, & Rioux, 2016; Hélou, Guandouz, & Aïmeur, 2012). Furthermore, the users’ perception of dating success is higher in online relationships than in the real-world (Fullwood & Attrill-Smith, 2017).

McKenna, Green, and Gleason (2002) make the argument that partners can be brought closer and become more intimate through online activities such as e-mailing, exchanging pictures, or chatting. They even suggest that a high level of intimacy can be achieved faster than in real-life face-to-face interactions. This might be because relationships formed on the Internet are based on criteria such as common interest, and are not biased by superficial ones such as the physical traits of the person.

Some research found that users’ engagement with social media contributes to tension and jealousy that far exceed offline relationship dynamics (Christofides, Muise, & Desmarais, 2009; Elphinston & Noller, 2011). In the first stages of dating, when people become “friends” on a social networking site, they are exposed to their partner’s profile, which may provide information about their budding romantic partner’s past that is not sensitively portrayed or contextualized (Fox, Osborn, & Warber, 2014). Because exchanges on social media are widely visible (due to the affordances of accessibility and visibility), romantic partners’ exchanges with others (who
may be threatening to the relationship) can also be viewed (Zurbriggen et al., 2016).

Similar works on online relationships deal with the impact of self-disclosure on the overall success of such relationships. Based on the reciprocity concept (Falk & Fischbacher, 2006), Jiang and colleagues (Jiang, Bazarova, & Hancock, 2013) studied the effect of reciprocity on self-disclosure in online relationships. They showed that text-based online relationships led to more reciprocity-based self-disclosure than face-to-face relationships did. Similarly, Kashian and colleagues (Kashian, Jang, Shin, Dai, & Walther, 2017; Lin & Utz, 2017) demonstrated that self-disclosure could lead to more liking and social attraction in online relationships (also known as computer-mediated communications). Social media users are more likely to get involved in an online relationship with someone who self-discloses to them.

The ease of creating and managing fake self-presentation, the increased reciprocity effect, and the tendency to self-disclose puts us in the front of an environment with high manipulation-related risks. Manipulation itself is a hard act to perceive as if the user feels that he/she has a choice in the decision, while in reality they are being led by the manipulator (Goldstein, 2015).

Manipulators count on people’s trust, doubt, and strong emotions to prevent them from thinking and acting clearly. Manipulation can be defined by the process that undermines the ability to consciously make decisions and take actions for the best by personal values and boundaries. In other words, manipulation gets people to do things they would not otherwise do. Even smart people can be trapped sometimes.

While privacy disclosure related to compromised social services is manageable, it becomes harder to control when the human factors behind it are considered. The privacy paradox states that users keep disclosing even when they are concerned. This has always been one of the most sensitive topics in privacy preservation. Giving the numerous technological solutions we possess, we still cannot meet the privacy preservation levels we expect. On the other hand, user-centric technological solutions may help social media users to protect their privacy by deliberately selecting their preferred privacy settings.

Consequently, we need to define the human factors behind privacy disclosure on social media and how we can mitigate their impact. To the best of our knowledge, while the related work focuses on mass deception through manipulative and fake information, very little research has been done to date to study the impact of manipulation on privacy in online relationships. For instance, the most relevant work done by Sharabi and colleagues studies the impact of using deception in a long-term relationship.
The authors based their study on the fact that users provide fake information to their online partner before the first physical meeting. However, the online relationship may quickly fail when the deception is discovered.

**Research model and hypotheses**

Considering the scenario from the introduction, we aim to explore the reasons behind the disclosure in online relationships. We start by identifying the different factors that may lead to such an issue, along with the possible links between each factor. To explore the reasons behind disclosure in online relationships, we start by identifying the factors that may lead to this issue. We then focus on factors related to specific cases such as online behavior and involvement in social interactions. The next step consists of identifying privacy-related factors that are affected by the ones defined in the previous step (e.g., privacy concerns, risk perception). The resulting factors are then organized according to the influence strength on disclosure in online relationships.

We discuss the theoretical background of each factor and their related hypotheses. The hypotheses are formulated as “X is positively related to Y” even when one factor might have the opposite effect on another (negative). In other words, the hypotheses are not expressed according to the logical effect of a factor (e.g., protection is positively related to cybersecurity versus protection is positively related to being hacked). We justify the use of similar effect directions for all hypotheses by the possible bias of study results when settings hypotheses according to background influences. Each factor is presented with its respective hypotheses in Figure 1.

**Hypotheses**

We discuss in this section our hypotheses and the theoretical background behind building each of them. Accordingly, we identify nine factors and their respective hypotheses from the literature.

**Trust**

This factor deals with the fact that the user’s trust toward social media and other users can significantly impact their willingness to disclose private information with an e-partner (see second section). This factor is adapted initially from work on knowledge sharing in virtual communities (Acquisti et al., 2015; Hsu, Ju, Yen, & Chang, 2007), measured according to two types of trust: information-based trust (INT) and identification-based trust (IDT).
Information-based trust (INT)
This factor is mainly related to adherence to technical standards, security procedures, and protection mechanisms (Ratnasingam, 2005). In other words, it arises when the technology infrastructures and control mechanisms meet the user’s security and privacy expectations. Moreover, INT is associated with a subjective perception of information-related security, and privacy protection mechanisms (Ba, 2001; Gefen, Karahanna, & Straub, 2003). Thus, INT in this study is defined as users’ trust in social media security and privacy protection mechanisms. The related hypotheses are:

H1.1. INT is positively related to privacy concerns in e-relationships.
H1.2. INT is positively related to the perceived risk in e-relationships.
H1.3. INT is positively related to the attitude toward manipulation.

Identification-based trust (IDT)
This stage of trust is developed when the different parties involved in a relationship (e.g. user–user relationship) reach a mutual understanding and can efficiently act for each other (Lander, Purvis, McCray, & Leigh, 2004; Lewicki & Bunker, 1995; McKnight & Chervany, 1996; McKnight, Choudhury, & Kacmar, 2002). IDT is related to the emotional commitments between individuals; it depends on how strongly developed are the relationships between them. In this study, IDT relies on social media users’ trust in different interaction among users. In other words, while IDT expands by knowing and predicting others’ needs and preferences, it also
allows us to think, feel and react like the other person (Lewicki & Bunker, 1995). The related hypotheses are:

**H2.1.** IDT is positively related to privacy concerns in e-relationships.

**H2.2.** IDT is positively related to the perceived risk in e-relationships.

**H2.3.** IDT is positively related to the attitude toward manipulation.

**Social interaction ties (SIT)**

Adapted from Chiu and colleagues’ work about the motivations behind people’s knowledge sharing in virtual communities (Chiu, Hsu, & Wang, 2006), this factor deals with the strength of the social ties among social media users. The strength of a social tie is often characterized by the amount of time, emotional intensity, mutual intimacy, and the common services between users (Granovetter, 1973). In this study, SITs are measured using the strength of relationships regarding the amount of time spent, along with the communication frequency between social media users. This choice is justified by the need for measured features and the relevance of these two properties to the context of online relationships. The related hypotheses are:

**H3.1.** SITs have a positive effect on privacy concerns in e-relationships.

**H3.2.** SITs have a positive effect on the perceived risk in e-relationships.

**H3.3.** SITs have a positive effect on the attitude toward manipulation.

**Risky online behavior (RBV)**

Adapted from the exploratory study of Walker and colleagues’ work on cyberbullying within undergraduate university students and the role of risky behavior in being vulnerable to such practices (Walker, Sockman, & Koehn, 2011). This factor deals with the impact of the user’s online behavior on the possibility of disclosing and exposing personal information. For instance, users who do not use privacy settings on social media networks, or expose their desires, inclinations, moods, or other information for anyone to see are considered users with risky online behavior. In this work, the different actions that can make a social media user exposed to security and privacy risks related to the context of online relationships (next section) are measured. Consequently, the related hypotheses are:

**H4.1.** The user’s risky behavior is positively related to privacy concerns in e-relationships.

**H4.2.** The user’s risky behavior is positively related to the perceived risk in e-relationships.
H4.3. The user’s risky behavior is positively related to his attitude toward manipulation.

**Privacy concerns in e-relationships (PCR)**
This factor deals with both, users’ concerns about the general privacy issues in social media, and privacy risks related to online relationships (Acquisti et al., 2015). We assume that low privacy concerns can lead to serious privacy leaks in online relationships. Consequently, the hypothesis related to this factor is:

**H5.** The lack of user privacy concerns has a positive effect on privacy disclosure in e-relationships.

**Perceived risk in e-relationships (PRR)**
Based on similar work on privacy risk perception (Drennan, Sullivan, & Previte, 2006), this factor considers user risk perception as a potential cause of privacy disclosure in e-relationships. We measure the user’s perception of overall privacy risks in social media, and the threats associated with being in an online relationship. The related hypothesis is:

**H6.** The perceived risk is positively related to privacy disclosure in e-relationships.

**Attitude toward manipulation (ATM)**
In its general meaning, this attitude is the tendency to support a particular condition, take a particular approach, or react in a particular way. In the case of manipulation, the attitude is represented by the reaction of an individual toward a manipulative behavior. In other words, an individual to be predisposed to manipulation when he/she does not act appropriately in some situations that may lead to him/her being manipulated (Kelman, 1965; Ma, Hancock, & Naaman, 2016; Skorbatyuk & Bazilevsky, 2015). To the best of our knowledge, this construct has not been studied before, and the assumptions we build are mainly based on the most relevant works from both psychology and sociology. This factor refers to people who trust others easily, who have doubts and strong emotions. When they experience difficult times, they become more vulnerable to manipulation.

**H7.** The ATM is positively related to privacy disclosure in e-relationships.

**Involvement in the e-relationship (IER)**
Adapted from a comparative study of the differences between romantic online and real-world relationships (Cornwell & Lundgren, 2001), this
factor, unlike social ties, deals with the strength of commitment of one individual to the online relationship, and its impact on privacy disclosure. In this study, this factor assesses the user’s engagement and its impact on their privacy. Similarly, we aim to compare the significant similarities and differences between a real world and an online relationship. In addition to the different relationship properties such as the period and meeting frequency, this factor is measured using three features: the user commitment to the relationship, their satisfaction about it, and its potential for growth. The related hypothesis is:

**H8.** The IER is positively related to the attitude toward manipulation.

**Research model**

To assess the effect of each factor, we evaluate two research models separately. Both models are based on the same set of factors, also known as constructs, and are used to differentiate users who previously had or currently are in an e-relationships and users who never got involved in one. Consequently, the only difference between the two models lies in the construct used to evaluate the involvement in the e-relationship. Moreover, the dataset should be divided into two groups, while the first one is used to measure the effect of the various factors when the user is involved in an e-relationship (“in-relationship” group), and the second model deals with the users who are not in an e-relationship (“no-relationship” group). Figure 1 illustrates the research model that we used. The “in-relationship” dedicated factor is illustrated by the dotted box.

**Methodology**

We discuss in this section the methodology used to evaluate the model from Figure 1. Given the type of model, we used structural equation modeling. Similarly, we discuss study goals and design, along with the survey administration and different encountered limitations.

**Study goals and design**

The first step of this study is evaluating the research model using Structural Equation Modeling (SEM). SEM consists of a diverse set of mathematical models, computer algorithms, and statistical methods that fit a research model built from constructs to a specific dataset (Boomsma, 2003). SEMs are used to assess unobserved constructs using observed variables. The evaluation of a given model starts by setting a measurement model that defines each unobserved variable using one or more observed
variables, and a structural model that imputes relationships between unobserved variables. The links between constructs of a SEM are considered as the research model hypotheses, and the values resulted after estimating each link loading evaluate each hypothesis. The estimated values are often calculated following the independent regression equations (Boomsma, 2003). Unlike simple correlation, independent regression equations are widely used in statistics to predict a potential relationship between dependent and independent variables (Cohen, Cohen, West, & Aiken, 2013). Concisely, SEM is the most suitable approach to evaluate research models built from constructs that cannot be evaluated without using other variables. An example from Figure 1 could be the construct of privacy concerns in e-relationships, it is clear that we cannot measure it directly; but with using questions related to privacy concerns, their answers are the values of variables employed to evaluate the construct under consideration. This approach was used in several similar studies (Aïmeur, Lawani, & Dalkir, 2016; Sahnoune, Aïmeur, El Haddad, & Sokoudjou, 2015) and yielded accurate findings. While the various factors are presented as unobserved variables, their construct items are used as observed variables and estimated using a survey. Thus, the second step, after setting the research model to SEM, consists of evaluating the constructs by conducting an online survey with numerous statement-based five-item scale questions when each of them represents an observed variable. The questions are adapted from other related and validated studies, and most of them were adopted to evaluate the same or similar unobserved variables.

Survey administration and limits

The survey was administered on Amazon’s Mechanical Turk (MTurk) platform in August 2015. MTurk workers (the name given to individuals who fill out questionnaires on MTurk) were invited to complete the survey for a compensation of $1.25. Workers were required to have the following qualifications: live in the United States or Canada, Human Intelligence Task (HIT) approval rate $\geq 95\%$, and some approved HITs $\geq 100$. The average completion time for the survey was 10 min, making the compensation consistent with payment standards of the MTurk community.

A total of 1,532 workers answered the questions. After data quality assessment, 17 were removed due to inadequate responses to eligibility questions and giving uniform answers to a large number of questions in a row. Hence, this study is based on the remaining 1,515 participants’ valid answers. Table 1 shows the self-reported demographic characteristics of the study sample.

Although MTurk can provide relevant results as any other traditional survey methods (Kittur, Chi, & Suh, 2008), its limitations cannot be
neglected. The main limitations when using the MTurk platform are the inability to control the experimental settings and the absence of robust support for participant assignment (Kittur et al., 2008). In other words, unlike traditional survey methods, we cannot manage the current environment of a participant as in traditional survey methods. Similarly, the options of the assignment of participants are somehow limited and do not allow a precise selection of the sample (e.g., age selection, marital status).

**Results and discussions**

Analysis of results began by examining the measurement model to test reliability and validity. Then the structural model was analyzed. More specifically, the recommended two-step approach (Anderson & Gerbing, 1988) was followed, and the analysis was performed using IBM SPSS Statistics 22, and IBM SPSS Amos 22 software. A Confirmatory Factor Analysis was performed first, testing convergent, and discriminant validity. While convergent validity defines if construct items can reflect their corresponding factor, discriminant validity ensures that the factors are statistically dissimilar.

We analyze the results according to two groups, the “in-relationship” group that contains the 504 participants who stated they had an intimate e-partner, and the “no-relationship” group that contains the remaining 1,011 participants. As mentioned earlier, we first examined the measurement model to assess reliability and validity for both the research model and the
Table 2. Summary of measurement scales.

| Construct | Measure | Mean | Std. dev. | Loading |
|-----------|---------|------|-----------|---------|
| **Information-based trust (INT) composite reliability: 0.846/0.818** | | | | |
| INT1 | Social media websites have enough safeguards to make me feel comfortable to divulge personal information. | 2.66 | 1.206 | 0.784 |
| INT2 | Social media users do not use personal information concerning their contacts for any purpose unless they have been authorized by the owner. | 2.47 | 1.183 | 0.740 |
| INT3 | Social media websites never sell personal information kept in their databases. | 2.10 | 1.242 | 0.802 |
| INT4 | Social media websites protect personal information from unauthorized access. | 2.72 | 1.095 | 0.727 |
| **Identification-based trust (IDT) composite reliability: 0.830/0.823** | | | | |
| IDT1 | I can talk freely to social media users about my personal issues. | 2.88 | 1.278 | 0.689 |
| IDT2 | If I share my problems with my contacts, I know they will help me. | 3.17 | 1.129 | 0.766 |
| IDT3 | I know that most contacts of my social media websites will do everything within their capacity to help others. | 2.92 | 1.149 | 0.765 |
| IDT4 | I know that most of my contacts on social media websites are honest. | 3.19 | 1.145 | 0.746 |
| **Social interaction ties (SIT) composite reliability: 0.788/0.808** | | | | |
| SIT1 | I maintain close social relationships with my contacts on social media websites. | 3.29 | 1.074 | 0.787 |
| SIT2 | I spend a lot of time interacting with some of my contacts on social media websites. | 3.30 | 1.214 | 0.775 |
| SIT3 | I know some of my social media contacts on a personal level. | 4.36 | 0.891 | 0.461 |
| SIT4 | I have frequent communication with some of my contacts on social media websites. | 3.92 | 1.025 | 0.729 |
| **Risky behavior (RBV) composite reliability: 0.701/0.804** | | | | |
| RBV1 | I posted something negative about myself online (intimate thoughts, worries, negative emotions, etc.). | 2.08 | 1.269 | 0.568 |
| RBV2 | I shared sensitive information online that later caused me problems. | 2.85 | 1.400 | 0.540 |
| RBV3 | I posted something online about others that got me in trouble. | 2.18 | 1.331 | 0.746 |
| RBV4 | I decided not to post something online because I was concerned that it might reflect badly on me in the future. | / | / | / |
| **Privacy concerns in e-relationships (PCR) composite reliability: 0.754/0.756** | | | | |
| PCR1 | I take measures to protect my data on social media websites. (inverted) | 4.15 | 0.941 | 0.630 |
| PCR2 | I make sure to use my social media websites on secured networks. (inverted) | 4.09 | 0.944 | 0.712 |
| **Perceived risk in e-relationships (PRR) composite reliability: 0.653/0.853** | | | | |
| PRR1 | Privacy policies protect my data on social media websites. (inverted) | 3.06 | 1.181 | 0.832 |
| PRR2 | The data on social media websites is sufficiently private. (inverted) | 3.24 | 1.093 | 0.839 |
| PRR3 | I discuss private family problems with my e-partner. (inverted) | 3.38 | 1.237 | 0.869 |
| PRR4 | My e-partner knows about my salary and other income information. (inverted) | 3.57 | 1.107 | 0.885 |
| **Attitude toward manipulation (ATM) composite reliability: 0.815/0.798** | | | | |
| ATM1 | It is hard for me to say “no” even when I know that it would be best for me to do so. | 2.65 | 1.345 | 0.638 |
| ATM2 | At the slightest conflict, I fear that all is over (with a friend or a loved one). | 2.47 | 1.330 | 0.756 |

(continued)
results. Table 2 shows each construct composite reliability, and the means, the standard deviations, and the loadings of each construct measure for the groups “in-relationship” and “no-relationship” accordingly.

As illustrated in Table 2, all the loadings are larger than 0.7 or slightly smaller in some cases; and all the composite reliability values are larger than 0.7. These values indicate good convergent validity (Bagozzi & Yi, 1988).

As illustrated in the research models, the “no-relationship” group estimates are evaluated without the “involvement in the e-relationship” construct, and the “disclosure in e-relationships” is evaluated using hypothetic statements. Table 6 shows all the constructs used and their respective discriminant validity values. We also follow the recommended two-step approach as for the previous group.

As listed in Table 6, all the loadings and the composite reliability value suggest a good convergent validity. The “disclosure in e-relationships” constructs were measured using the following hypothetical statements:

**Statement 1:** Consider the following statement and answer appropriately: "Two e-partners, Alice and Bob, are in a close personal e-relationship. Bob asks Alice for her Facebook password and Skype contact list. Alice answers yes, and gives Bob this private information."

**Question:** Agreement scale on Alice behavior.

**Statement 2:** Consider the following statement and answer appropriately:

Before giving her private information, Alice performed an in-depth clean-up of messages and contact lists, and started to monitor her social media activities;
periodically. She has also warned some of her contacts about the situation, and has even created parallel accounts with fake identities.

**Question 1:** Agreement scale on performing a clean-up.

**Question 2:** Agreement scale on monitoring social media activities.

The next step is the evaluation of the discriminant validity by comparing for each construct, the square root of its average variance extracted (AVE) and its correlation coefficients with other constructs.

As illustrated in Table 3 and Table 4, all AVEs are greater than the recommended value which is 0.5 and the square of each construct is bigger than any of its correlation coefficient with other constructs.

**Table 3.** The AVE, the square root of AVE (shown as bold) and factor correlation coefficients for the “in-relationship group.”

|      | AVE | INT  | IDT  | SIT  | RBV  | PCR  | PRR  | ATM  | DER  | IER  |
|------|-----|------|------|------|------|------|------|------|------|------|
| INT  | 0.846 | 0.761 | | | | | | | | |
| IDT  | 0.830 | 0.700 | 0.742 | | | | | | | |
| SIT  | 0.788 | 0.362 | 0.628 | 0.701 | | | | | | |
| RBV  | 0.384 | 0.377 | 0.375 | 0.231 | 0.619 | | | | | |
| PCR  | 0.754 | −0.123 | −0.072 | −0.043 | 0.059 | 0.783 | | | | |
| PRR  | 0.653 | 0.912 | 0.603 | 0.226 | 0.282 | −0.189 | 0.623 | | | |
| ATM  | 0.815 | 0.294 | 0.287 | 0.182 | 0.579 | 0.118 | 0.280 | 0.690 | | |
| DER  | 0.624 | 0.503 | 0.354 | 0.129 | 0.605 | 0.032 | 0.428 | 0.375 | 0.675 | |
| IER  | 0.794 | 0.284 | 0.315 | 0.308 | 0.078 | −0.210 | 0.361 | 0.123 | 0.312 | 0.752 |

**Note.** AVE = average variance extracted; INT = information-based trust; IDT = identification-based trust; SIT = social interaction ties; RBV = risky behavior; PCR = privacy concerns in e-relationships; PPR = Perceived risk in e-relationships; ATM = attitude toward manipulation; DER = disclosure in e-relationships; IER = involvement in the e-relationships.

**Table 4.** The AVE, the square root of AVE (shown as bold) and factor correlation coefficients for the “no-relationship” group.

|      | AVE | INT  | IDT  | SIT  | RBV  | PCR  | PRR  | ATM  | DER  | IER  |
|------|-----|------|------|------|------|------|------|------|------|------|
| INT  | 0.530 | 0.728 | | | | | | | | |
| IDT  | 0.540 | 0.612 | 0.735 | | | | | | | |
| SIT  | 0.521 | 0.373 | 0.627 | 0.722 | | | | | | |
| RBV  | 0.586 | 0.139 | 0.125 | 0.122 | 0.765 | | | | | |
| PCR  | 0.609 | −0.050 | −0.031 | 0.000 | 0.142 | 0.780 | | | | |
| PRR  | 0.744 | 0.909 | 0.568 | 0.399 | 0.083 | −0.147 | 0.862 | | | |
| ATM  | 0.453 | 0.142 | 0.096 | 0.067 | 0.402 | 0.229 | 0.079 | 0.673 | | |
| DER  | 0.758 | −0.127 | −0.012 | 0.036 | −0.127 | −0.090 | −0.122 | 0.018 | 0.871 | |

**Table 5.** The actual values of model fitness indices.

| Model fit indices | Results (in-relationship) | Results (no-relationship) | Recommended value |
|-------------------|---------------------------|---------------------------|-------------------|
| Chi-square statistic (χ²/df) | 3.53 | 4.73 | ≤ 5 |
| Normed Fit Index (NFI) | 0.792 | 0.910 | ≥ 0.8 |
| Comparative Fit Index (CFI) | 0.840 | 0.924 | ≥ 0.9 |
| Root Mean Square Error of Approximation (RMSEA) | 0.071 | 0.071 | ≤ 0.08 |

**Note.** AVE = average variance extracted; INT = information-based trust; IDT = identification-based trust; SIT = social interaction ties; RBV = risky behavior; PCR = privacy concerns in e-relationships; PRR = Perceived risk in e-relationships; ATM = attitude toward manipulation; DER = disclosure in e-relationships.
Accordingly, this proves a good discriminant validity (Bagozzi & Yi, 1988).

Before addressing the estimated values and the hypotheses tests, we list the model fitness indices in Table 5, which illustrates the ratio between Chi-square and the degree of freedom (<3 good, <5 permissible; Satorra & Bentler, 2001); Bentler and Bonett’s Normed Fit Index (NFI) which considered to be good for value greater than 0.80 (Bentler & Bonett, 1980); the Comparative Fit Index (CFI), good when greater than 0.90 (Bentler & Bonett, 1980); and the Root Mean Square Error of Approximation
Table 6. Hypotheses test results (N.S.: Not supported due the large \( p \)-value).

| Attributes | Est. | \( p \)-value | Hypo. status | Attributes | Est. | \( p \)-value | Hypo. status |
|------------|------|---------------|--------------|------------|------|---------------|--------------|
| INT \( \rightarrow \) PCR | -0.400 | 0.002 | H1.1 Supported | RBV \( \rightarrow \) PCR | 0.648 | <0.001 | H4.1 Supported |
| INT \( \rightarrow \) PRR | -0.958 | <0.001 | H1.1 Supported | / | / | H4.2 Invalid |
| INT \( \rightarrow \) ATM | 0.056 | 0.156 | N.S. | RBV \( \rightarrow \) ATM | 0.996 | <0.001 | H4.3 Supported |
| IDT \( \rightarrow \) PCR | / | / | H2.1 Invalid | IER \( \rightarrow \) PCR | -0.648 | <0.001 | H8.1 Supported |
| IDT \( \rightarrow \) PRR | -0.135 | <0.001 | H2.2 Supported | IER \( \rightarrow \) PRR | -0.189 | <0.001 | H8.2 Supported |
| IDT \( \rightarrow \) ATM | -0.068 | 0.03 | H2.2 Supported | / | / | / |
| SIT \( \rightarrow \) PCR | / | / | H3.1 Invalid | PCR \( \rightarrow \) DER | -0.425 | 0.025 | H5 Supported |
| SIT \( \rightarrow \) PRR | 0.170 | <0.001 | H3.2 Supported | PRR \( \rightarrow \) DER | -0.407 | 0.003 | H6 Supported |
| SIT \( \rightarrow \) ATM | -0.071 | 0.072 | H3.3 Supported | ATM \( \rightarrow \) DER | 0.970 | <0.001 | H5 Supported |
| SIT \( \rightarrow \) ATM | -0.061 | 0.044 | H3.3 Supported | / | / | / |

Note. INT = information-based trust; PCR = privacy concerns in e-relationships; PRR = Perceived risk in e-relationships; ATM = attitude toward manipulation; RBV = risky behavior; IER = involvement in the e-relationships; DER = disclosure in e-relationships.

(RMSEA) which is recommended to be smaller than 0.08 (Hancock & Freeman, 2001; Ullman & Bentler, 2012).

Finally, the estimates of our research model were calculated and are illustrated in Figure 2 for the “in-relationship” group, and in Figure 3 for the “no-relationship” group. Accordingly, Table 6 lists results for both groups. Some of the assertions are not supported due to either the low value of estimate or invalid because of the high \( p \)-value (>0.1). Accordingly, the disclosure in e-relationship is mainly impacted by the attitude toward manipulation.

**Discussion and findings**

The estimated values obtained in the previous section suggests several conclusions, especially concerning the factors that affect disclosure in e-relationships and those affecting the attitude toward manipulation (attitude of vulnerability to manipulation). We first discuss the significant findings that both the “in-relation” and “no-relation” groups have in common. Then, we summarize the key differences between both groups and discuss the specific findings of each.

**Common findings**

Among the key findings of the estimated results, some interfactor relations were similar in both groups. Although the estimated values were slightly different, they led to the same interpretations.
The main factor affecting data disclosure in e-relationships is the attitude toward manipulation (H8).

The user’s attitude toward manipulation is mainly affected by his/her online behavior (H4.3). Users with risky online behavior are more susceptible to online manipulation.

Regardless of the user’s privacy concerns or risk perception, his/her risky online behavior is the main cause behind disclosure in online relationships.

The risky online behavior, which is positively related to the attitude toward manipulation, is also positively related to privacy concerns (H4.1). In particular, even when a user may be concerned about privacy, he/she still adopts risky online behavior, and consequently, is more exposed to the attitude toward manipulation. This also suggests that the attitude toward manipulation does not depend on user privacy concerns or risk perception. Another point that confirms this claim is the invalid hypothesis as perceived risk is related to risky online behavior. The estimated value of the user’s risky online behavior and privacy concerns also suggests that the user’s online behavior and privacy-related attitudes are somehow independent.

The other common estimates are the negative relations between INT and both privacy concerns (H1.1) and risk perception (H1.2). These two hypothesis values confirm the results of previous work about privacy concerns (Aïmeur, Lawani, et al., 2016) and assert the independence of disclosure privacy-related attitudes in the context of e-relationships.

The perceived risk in online relationships is positively related to the users’ social interaction ties (H3.2).

**Specific findings**

Along with common findings, each group’s model estimates suggest other specific findings. Table 7 lists the differences between each group, even when the hypotheses under consideration are the same. Specifically, some estimates differ in the two groups, but these are because users are not in an e-relationship. One notable finding suggested by the results lies in the
dependency of the attitude toward disclosure on being in an online relationship. While most users from the “no-relation” group disagree with the disclosure statements from before, the majority of users in the “in-relation” group disclose private information when asked for it. This statement can be explained by the fact that nearly 85% of the users have an online relationship and when their e-partners asked for private credentials they had already shared them. In other words, being in an e-relationship can seriously affect the user concerns about privacy. This suggests that being involved in an online relationship can change the user’s perception of privacy, online behavior, and eventually attitude toward manipulation.

**Further analyses**

Additional analyses were performed to explore critical aspects of the participants’ points of view. Each section from the survey ended with an optional open question that allowed participants to give their opinions and explanations about disclosure in e-relationships. We received a total number of 259 comments from participants who did not agree to share private information with e-partners, and 84 from those who did agree. In summary, some social media users believe that it is all about trust, and sharing private information helps in building that trust. Others treat long-term personal online relationships much like real life relationships and think that they do not have to hide anything from the other person, and do not mind having them know the details of their lives.

However, one important finding from the comments was that users who are normally careful in real life where they do not display risky behavior do end up disclosing their credentials to please their e-partners or to have peace in their relationships. In fact, among the 204 participants without risky behavior, 72 already gave up their online credentials. More formally, the impact of the involvement on the e-relationship on the disclosure is estimated to be 0.36 for users without risky online behavior. This value suggests a significant link between being involved and disclosing personal information to e-partners, even among vigilant users. The addition, an e-relationship not only has an impact on the privacy of the person but also endangers his or her relations and friends. The amount and the sensitivity of the information that the manipulator may obtain could lead to severe consequences to multiple individuals.

**Conclusion**

In conclusion, the findings of this work show that people who are committed to online relationships and exhibit risky behavior are more likely to divulge confidential information. Beyond their self-disclosure, they disclose
information about others in social network websites (Koohikamali, Peak, & Prybutok, 2017). They trust their online relationships and reveal confidential or sensitive information regardless of their privacy concerns or risk perception. Some users admit that they eventually disclose private information in a moment of weariness. This is something that may be repaired in real life, but not necessarily in a pervasive environment in which information spreads and quickly becomes uncontrollable, as on social media.

Social media foster happiness as well as unhappiness, sincerity as well as manipulation, but everything is magnified tenfold, facilitated by anonymity and by the absence of visual cues such as facial expressions and feelings. Once a virtual emotional connection is established, meeting in real life may take place. In that case, manipulation can occur if one confuses the real person with all the panache that he or she had created from his or her computer screen. Moreover, human needs have not changed, and the psychological needs as described in the pyramid of Maslow (Maslow, 1943) are fulfilled with or without online services. However, the privacy costs that one may bear are much heavier in an online world, where information is so easily spread.

Social media users have a social responsibility and need to ensure that their behavior does not infringe upon their privacy or that of others. Moreover sharing personal information with others makes them the co-owners of that information (Moon, 2000). It is important to reconsider privacy awareness among social media users. Proper awareness and training can go a long way toward reducing the risk of users revealing confidential information online. However, no privacy policy can be truly effective unless users know about it and understand the importance of following it and the consequences of not following it (Solove & Citron, 2017). “Although such influence is not always or necessarily malevolent or dangerous, relinquishing control over one’s data and one’s privacy alters the balance of power between those holding the data and those who are the subjects of that data” (Acquisti et al., 2015).

This work contributes to a better understanding of intentional disclosure in online relationships, characterized by one-on-one communications, and the impact of disclosure behavior on interpersonal relationships in social media. Similarly, we believe that the findings of this article constitute a major step toward understanding online deception and provide a solid theoretical background for future work in this regard. Online deception (Grace & Leskovicha, 2015; Lee & Wright, 2016; Tsikerdekis & Zeadally, 2014) represents one of the recent research areas that need collaborative efforts of psychology, sociology, and computer science. The costs of deception related to social media environments lead to several technical challenges that both developers and users must address.

The results of this work show a significant impact of attitudes toward manipulation on intentional disclosure in online relationships. Individuals
are willing to reveal sensitive information to people that they have never met. While promising, the results presented in this article need to be investigated further using programmed chatbots to estimate the disclosure level is one track that may improve our understanding of such situations.

Similarly, the reasons behind disclosure in online relationships deserve more exploration. Everyone is influenced by the environment, social interactions, and the life experiences they have had (Eriksson, 2017). Therefore, we intend to study additional factors that could affect the attitude toward manipulation itself, such as what can lead people to accept manipulation and eventually disclose their online credentials. This could span a wide range of possibilities between being toxically addicted to the manipulator to simply wanting peace. Additionally, we intend to perform an in-depth multigroup analysis on each predefined group in order to determine the main differences between users having different gender, age, or educational backgrounds. Manipulators have dangerous personalities (Navarro & Poynter, 2014) and it is important to learn how to identify them on social media. One straightforward, yet delicate approach could be the use of profiling techniques to identify these “dangerous personalities.” Effective psychological profiling is a challenge in itself (Bloom, 2013), and using it to identify online manipulators requires even more effort. Finally, 20 years ago already, the Massachusetts Institute of Technology’s Media Lab director, Nicholas Negroponte, stated that “Computing is not about computers anymore, it is about living”; imagine what he would have said today …

Acknowledgment
This work was partially supported by the Natural Sciences and Engineering Research Council of Canada.

ORCID
Zakaria Sahnoune http://orcid.org/0000-0003-2990-265X

References
Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science (New York, N.Y.), 347(6221), 509–514.  
Aïmeur, E., Brassard, G., & Rioux, J. (2013). Data privacy: An end-user perspective. International Journal of Computer Networks and Communications Security, 1(6), 237–250.  
Aïmeur, E., Brassard, G., & Rioux, J. (2016). CLiKC: A privacy-mindful approach when sharing data. Paper presented at the International Conference on Risks and Security of Internet and Systems.
Aïmeur, E., Lawani, O., & Dalkir, K. (2016). When changing the look of privacy policies affects user trust: An experimental study. *Computers in Human Behavior, 58*, 368–379.

Altman, I., & Taylor, D. A. (1973). *Social penetration: The development of interpersonal relationships*. New York: Holt, Rinehart & Winston.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411–423.

Ba, S. (2001). Establishing online trust through a community responsibility system. *Decision Support Systems, 31*(3), 323–336.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74–94.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). Retrieved from https://firstmonday.org/ojs/index.php/fm/article/view/1394/1312

Bentler, P. M., & Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin, 88*(3), 588–606.

Bloom, R. (2013). *Foundations of psychological profiling: Terrorism, espionage, and deception*. Boca Raton, FL: CRC Press.

Boomsma, A. (2003). Structural equation modeling: Foundations and extensions (Advanced Quantitative Techniques in the Social Sciences Series, Vol. 10.) by David Kaplan. *Structural Equation Modeling, 10*(2), 323–331.

Bradbury, D. (2015). The kids are alright [social media]. *Engineering & Technology, 10*(1), 30–33.

Chiu, C.-M., Hsu, M.-H., & Wang, E. T. (2006). Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories. *Decision Support Systems, 42*(3), 1872–1888.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: are they two sides of the same coin or two different processes? *CyberPsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society, 12*(3), 341–345.

Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2013). *Applied multiple regression/correlation analysis for the behavioral sciences*. London: Routledge.

Coons, C., & Weber, M. (2014). *Manipulation: theory and practice*. Oxford: Oxford University Press.

Cornwell, B., & Lundgren, D. C. (2001). Love on the Internet: Involvement and misrepresentation in romantic relationships in cyberspace vs. realspace. *Computers in Human Behavior, 17*(2), 197–211.

Cosby, P. C. (1973). Self-disclosure: A literature review. *Psychological Bulletin, 79*(2), 73–91.

Drennan, J., Sullivan, G., & Previte, J. (2006). Privacy, risk perception, and expert online behavior: An exploratory study of household end users. *Journal of Organizational and End User Computing (Computing), 18*(1), 1–22.

Ebner, N. C., Ellis, D. M., Lin, T., Rocha, H. A., Yang, H., Dommaraju, S., …, Spreng, R. N. (2018). Uncovering susceptibility risk to online deception in aging. *The Journals of Gerontology: Series B*. doi:10.1093/geronb/gby036

Elphinston, R. A., & Noller, P. (2011). Time to face it! Facebook intrusion and the implications for romantic jealousy and relationship satisfaction. *Cyberpsychology, Behavior, and Social Networking, 14*(11), 631–635.

Eriksson, M. V. (2017). *Manipulation: 12 dangerous persuasion secrets used by the world’s most powerful men to manipulate, persuade & influence people*. Scotts Valley, CA: CreateSpace Independent Publishing Platform.
Falk, A., & Fischbacher, U. (2006). A theory of reciprocity. *Games and Economic Behavior, 54*(2), 293–315.

Fox, J., Osborn, J. L., & Warber, K. M. (2014). Relational dialectics and social networking sites: The role of Facebook in romantic relationship escalation, maintenance, conflict, and dissolution. *Computers in Human Behavior, 35*, 527–534.

Fullwood, C., & Attrill-Smith, A. (2017). Up-dating: ratings of perceived dating success are better online than offline. *Cyberpsychology, Behavior, and Social Networking, 21*(1), 11–15.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51–90.

Goldstein, E. (2015). *Social engineering: The art of deception, psychological warfare, and mind manipulation*. Scotts Valley, CA: CreateSpace Independent Publishing Platform.

Grace, R., & Leskovicha, R. (2015). Challenges in the use of social media data for the next generation analyst. In *Proceedings Volume 9499, Next-Generation Analyst III*; p. 949903.

Granovetter, M. S. (1973). The strength of weak ties. *American Journal of Sociology, 78*(6), 1360–1380.

Hancock, G. R., & Freeman, M. J. (2001). Power and sample size for the root mean square error of approximation test of not close fit in structural equation modeling. *Educational and Psychological Measurement, 61*(5), 741–758.

Hélon, C., Guandouz, A., & Aimeur, E. (2012). A privacy awareness system for facebook users. *Journal of Information Security Research, 31*, 15–29.

Hsu, M.-H., Ju, T. L., Yen, C.-H., & Chang, C.-M. (2007). Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. *International Journal of Human-Computer Studies, 65*(2), 153–169.

Jiang, L. C., Bazarova, N. N., & Hancock, J. T. (2013). From perception to behavior: Disclosure reciprocity and the intensification of intimacy in computer-mediated. *Communication Research, 40*(1), 125–143.

Jourard, S. M., & Lasakow, P. (1958). Some factors in self-disclosure. *Journal of Abnormal Psychology, 56*(1), 91–98.

Kashian, N., Jang, J-W., Shin, S. Y., Dai, Y., & Walther, J. B. (2017). Self-disclosure and liking in computer-mediated communication. *Computers in Human Behavior, 71*, 275–283.

Kelman, H. C. (1965). Manipulation of human behavior: An ethical dilemma for the social scientist. *Journal of Social Issues, 21*(2), 31–46.

Kittur, A., Chi, E. H., & Suh, B. (2008). Crowdsourcing user studies with Mechanical Turk. Paper presented at the Proceedings of the SIGCHI conference on human factors in computing systems.

Koohikamali, M., Peak, D. A., & Prybutok, V. R. (2017). Beyond self-disclosure: Disclosure of information about others in social network sites. *Computers in Human Behavior, 69*, 29–42.

Lander, M. C., Purvis, R. L., McCray, G. E., & Leigh, W. (2004). Trust-building mechanisms utilized in outsourced IS development projects: A case study. *Information & Management, 41*(4), 509–528.

Lee, M., & Wright, E. (2016). Ethical issues in (Online) social network research in education. *Journal of Cyber Education, 10*(1), 9–14.

Lewicki, R. J., & Bunker, B. B. (1995). Trust in relationships. *Administrative Science Quarterly, 5*, 583–601.

Lin, R., & Utz, S. (2017). Self-disclosure on SNS: Do disclosure intimacy and narrativity influence interpersonal closeness and social attraction? *Computers in Human Behavior, 70*, 426–436.
Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers’ use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 10(3), 393–411.

Ma, X., Hancock, J., & Naaman, M. (2016). Anonymity, intimacy and self-disclosure in social media. Paper presented at the Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. New York: ACM.

Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, 50(4), 370–396.

McKenna, K. Y., Green, A. S., & Gleason, M. E. (2002). Relationship formation on the Internet: What’s the big attraction? *Journal of Social Issues*, 58(1), 9–31.

McKnight, D. H., & Chervany, N. L. (1996). The meanings of trust. Minneapolis, MN: Carlson School of Management, Univ. of Minnesota.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334–359.

Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research*, 26(4), 323–339.

Navarro, J., & Poynter, T. S. (2014). Dangerous personalities: An FBI profiler shows you how to identify and protect yourself from harmful people. Emmaus, PA: Rodale.

Petronio, S. (2012). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: Suny Press.

Ratnasingam, P. (2005). Trust in inter-organizational exchanges: a case study in business to business electronic commerce. *Decision Support Systems*, 39(3), 525–544.

Sahnoune, Z., Aimeur, E., El Haddad, G., & Sokoudjou, R. (2015). Watch your mobile payment: An empirical study of privacy disclosure. Paper presented at the Trustcom/BigDataSE/ISPA, 2015 IEEE.

Satorra, A., & Bentler, P. M. (2001). A scaled difference chi-square test statistic for moment structure analysis. *Psychometrika*, 66(4), 507–514.

Sharabi, L. L., & Caughlin, J. P. (2018). Deception in online dating: Significance and implications for the first offline date. *New Media & Society*, 21(1), 229–247.

Singh, N., Sharma, T., Thakral, A., & Choudhury, T. (2018). Detection of fake profile in online social networks using machine learning. Paper presented at the 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE).

Skorbatyuk, O., & Bazilevsky, K. (2015). *Human manipulation modes: Either you are manipulating or you are being manipulated*, Vol. 3. San Diego, CA: HPA Press.

Solove, D. J., & Citron, D. (2017). Risk and anxiety: A theory of data breach harms. *Texas Law Review*, 96, 738–787.

Stein, L., & Sinha, N. (2002). New global media and communication policy: the role of the state in the twenty-first century. In *Handbook of new media: Social shaping and consequences of ICTs* (pp. 410–431). London: Sage.

Taylor, D. A., & Altman, I. (1966). Intimacy-scaled stimuli for use in studies of interpersonal relations. *Psychological Reports*, 19(3), 729–730.

Taylor, D. A., Altman, I., & Sorrentino, R. (1969). Interpersonal exchange as a function of rewards and costs and situational factors: Expectancy confirmation-disconfirmation. *Journal of Experimental Social Psychology*, 5(3), 324–339.

Tsikerdekis, M., & Zeadamente, S. (2014). Online deception in social media. *Communications of the Acm*, 57(9), 72–80.

Ullman, J. B., & Bentler, P. M. (2012). Structural equation modeling. In *Handbook of psychology* (2nd ed.). New York: Wiley.
Van der Walt, E., Eloff, J. H., & Grobler, J. (2018). Cyber-security: Identity deception detection on social media platforms. *Computers & Security, 78*, 76–89.

Walker, C. M., Sockman, B. R., & Koehn, S. (2011). An exploratory study of cyberbullying with undergraduate university students. *TechTrends, 55*(2), 31–38.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review, 25*(1), 166.

Zurbriggen, E. L., Ben Hagai, E., & Leon, G. (2016). Negotiating privacy and intimacy on social media: Review and recommendations. *Translational Issues in Psychological Science, 2*(3), 248–260.