International Journal of Communication 14(2020), 3704–3726 1932–8036/20200005

A Model of Social Eavesdropping in Communication Networks

LEILA BIGHASH
University of Arizona, USA

KRISTEN S. ALEXANDER
CHRISTINA S. HAGEN
ANDREA B. HOLLINGSHEAD
University of Southern California, USA

Social eavesdropping is the gathering of information from the interactions of 2 or more people, without their expressed knowledge or expressed permission, by a third party who is ostensibly not the target audience. Grounded in uncertainty management, communication networks, and signaling theories, this article presents a theoretical framework for understanding when and how individuals are likely to eavesdrop on the interactions of others. Social eavesdropping can be actively premeditated or passively incidental, the latter spurred by a serendipitous encounter. Propositions derived from the model investigate how accessibility, information value, and social risk influence the likelihood of social eavesdropping.

Keywords: surveillance, organizational communication, communication networks, uncertainty management, information gathering, privacy

Information gathering is essential for people, whether at home, in social situations, or in the organizations around which so much of daily life revolves. In organizations, for example, newcomers gather information to become socialized in new organizational cultures, learning norms and routines critical for success (Kramer, 2010). Managers gather information to inform their decisions and direct their subordinates (Anderson, 2008; Choo, 2001). However, not all information-gathering behaviors are equal. The following example highlights a specific type of behavior we seek to define and conceptualize.

Lyndsay Kirkham sat down for lunch at a restaurant in Toronto when she serendipitously overheard a group of IBM executives at a nearby table candidly discussing their sexist hiring practices. She live-Tweeted commentary about the presumably private conversation while eavesdropping (e.g., "These IBM

Leila Bighash: lbighash@email.arizona.edu
Kristen S. Alexander: steves@usc.edu
Christina S. Hagen: chagen@usc.edu
Andrea B. Hollingshead: aholling@usc.edu
Date submitted: 2019–11–01

executives should have picked someone else to sit beside to have a working lunch focused on 'why they don't hire women'" (Kirkham, 2014, as cited in Romano, 2014, para. 3). A firestorm of Tweets, blogs, and media coverage ensued, resulting in a public relations nightmare for the company (Williams, 2014).

This case is an example of social eavesdropping, defined as the gathering of information from the interactions of two or more people, without their expressed knowledge or expressed permission, by a third party or bystander who is ostensibly not the target audience. This communication behavior extends across people, cultures, contexts, and time (Locke, 2010) as well as species, which is evidenced by studies on the eavesdropping behavior of primates, birds, fish, and more (Cheney & Seyfarth, 2005; Magrath, Haff, Fallow, & Radford, 2015).

Social eavesdropping is a common behavior. For example, as Goffman (1979) states, "[Bystanders'] presence should be considered the rule, not the exception" (p. 8). Mass and social media discourse surrounding eavesdropping is prevalent. A recent Reddit discussion forum post and thread titled "What's the strangest conversation you've 'accidentally' eavesdropped on?", for instance, was exceptionally popular (receiving about six thousand comments[1]), with many comments relating to eavesdropping experiences in organizations or at work (LeggyBald, 2019).

However, social eavesdropping among people is not well understood. While Goffman (1979) discussed eavesdropping in his work on participation in conversations, social science research has yet to empirically and theoretically explore the antecedents of eavesdropping behavior. Social eavesdropping is a method of information gathering that enables individuals to be unratified participants (i.e., someone who is in range of an encounter, but is not an official participant in the encounter) in others' conversations (Goffman, 1979), sometimes unknown to those who are sending and receiving messages. It is important for communication scholars to theorize about eavesdropping as a unique, information-gathering method because, like those exploring information management implicitly suggest, sometimes targets from which there is interest in obtaining information are dishonest or ineffective at conveying their messages directly (Afifi & Weiner, 2004). A faulty assumption in information management scholarship, however, is that if targets are unable or unwilling to share honest information, individuals will not seek information from said targets (Afifi & Weiner, 2004, p. 179). Alternatively, we contend that when individuals want information from these targets, they may eavesdrop rather than stop their search or engage their targets directly.

There are many reasons to eavesdrop rather than gather information in other ways. Information gathered through social eavesdropping may be more honest or unique than that gathered through direct interaction. Social eavesdropping may be less risky and costly than other forms of information gathering. It may also result in a "second-order" information advantage, in which the interactants are unaware the eavesdropper knows what they know. As such, we argue that social eavesdropping is unique and warrants attention.

[1] One study found that Reddit posts received an average of 54 comments, and half received fewer than 10 comments in their data set (Weninger, 2014).

The goals of this article are twofold. First, we define social eavesdropping and examine each component of that definition. Second, we propose a conceptual model of social eavesdropping that can be applied across communication contexts. We conclude with implications of this model and directions for future research.

Social Eavesdropping Defined

In ancient cooperative hunter-gatherer societies, open living and awareness of others were necessary to maintain harmony (Locke, 2005, 2010). When societies moved to more domesticated hierarchies, however, walls and other privacy boundaries were constructed, leading to shifts in information sharing and gathering behavior. The English word "eavesdropper" is a product of this historical transition, referring to a person who secretly listens from under the roof or eaves of a house ("Eavesdrop," n.d.).

We restrict our theorizing to social eavesdropping, the scope of which is bound in several ways. First, we limit our examination to eavesdropping in which individuals gather information from the interactions between two or more people—thus, the term "social." This behavior excludes watching, monitoring, or listening to lone individuals.[2] The term "social" is also used because eavesdropping often has a negative connotation and stigma. We propose that social eavesdropping is not always unethical; in fact, we argue it may be prosocial in some cases. For example, preschoolers listen in on their peers' questions and subsequent responses, helping them to learn and solve problems on their own (Mills, Danovitch, Grant, & Elashi, 2012). Although the question-asking preschoolers and teachers may be aware of others listening in, they have not expressed their knowledge or permission to these bystanders; thus, this case adheres to the definition of social eavesdropping.

Second, we focus on the eavesdropper rather than those involved in the interactions being eavesdropped on (i.e., the communicators or interactants). Like previous work exploring uncertainty (Brashers, 2001) and information management (Afifi & Weiner, 2004), we recognize the importance of the interactants in social eavesdropping. Interactants play a key role in the communication network, provide cues to eavesdroppers, and coordinate privacy boundaries with one another. Interactants navigate potential boundary turbulence (i.e., when privacy rules are misunderstood or violated) if the eavesdropper becomes known (Petronio, 2002). To bound and define the scope of this work, however, we focus on social eavesdroppers and only consider the interactants in relation to the actions of eavesdroppers. Eavesdroppers play critical roles in both the structure of the network and ownership of information because eavesdroppers create new ties and gain new information, possibly covertly. Interactants may or may not be aware of information-gathering by eavesdroppers.

Lastly, we limit the definition of social eavesdropping to processes that involve acquiring information from the interactions of others without their expressed knowledge or expressed permission. In a communication network, the eavesdropper is a third party or bystander who is ostensibly not the target audience, although they are connected to the interactants through information flow ties. This definition does not imply interactants are necessarily unaware of the third party—rather, their knowledge or permission is

[2] Monitoring lone individuals may provide equally important information; this type of behavior is simply outside the scope of the definition of social eavesdropping.

not expressly stated or communicated to the eavesdropper. In the following sections, we elaborate on the defining elements of social eavesdropping: (a) information gathering, (b) interactions of two or more people, and (c) third parties in communication networks.

Information Gathering

Social eavesdropping involves gathering information from social interactions. It is considered an information-seeking tactic (Morrison, 1993) and a socially adaptive learning strategy (BliegeBird et al., 2005; Peake, 2005). Previous information-seeking literature focuses primarily on purposeful behavior like source selection (Berger, 2002). Our model assumes that information gathering can be either intentional or incidental.

Active social eavesdropping is defined as a purposive behavior to encounter an interaction between other actors (Bates, 2002; Savolainen, 2016). Goffman (1979) explains that this involves those who "engineer" an encounter where they can listen in on others' conversations. On the other hand, passive or serendipitous (Case & Given, 2016) social eavesdroppers encounter a social interaction through unplanned and incidental circumstances, equivalent to overhearers in Goffman's (1979) terms. We acknowledge that others in the communication discipline use the terms "active" and "passive" differently than how they are employed in this article. For example, Berger (2002) treats both passive and active information acquisition as strategic, and cognitively disengaged information acquisition as nonstrategic. We avoid the term "strategic" because regardless of whether an encounter is actively planned or passively discovered, communication of any kind, including automated or unconscious communication, is always goal driven (Kellermann, 1992). As such, we adopt information science's use of the terms "active" and "passive."

Many scholars acknowledge the possibility of "unintentional communication" (Williamson, 1998), ranging from passive strategies that avoid social interaction (Berger, 2002) to accidental encounters with information that spark new or preexisting interests or needs (Case & Given, 2016). An accidental encounter occurs, for example, when a parent notices and reads an incoming text on their teenager's unattended phone. Hsieh (2009) found that eavesdropping is typically unplanned or passive, resulting in accidental knowledge in a workplace setting. On finding an interesting topic or source of information, once-serendipitous eavesdroppers may become active eavesdroppers during the same or related encounters with interactants, highlighting the dynamic and temporal nature of social eavesdropping processes and mechanisms.

Information gained through social eavesdropping can be used for functional purposes, such as to improve efficiency, locate resources, avoid threats, and achieve other forms of personal or communal gain (Peake, 2005). It can also serve as entertainment (Locke, 2010). For example, there are Instagram accounts devoted to posting eavesdropped conversations from different locations like Los Angeles, New York, universities, and even Uber rides, among others (e.g., @overheardla; Varian, 2019).

In addition to information from the messages exchanged between interactants, social eavesdroppers can gather information about the interacting people themselves and their relationships, such as affiliation and relational status (BliegeBird et al., 2005; Cheney & Seyfarth, 2005; Donath, 2007; Peake,

2005). Eavesdroppers extract information by attending to signals such as message content, tone of voice, emotional state, and body language (Donath, 2007). They can also make inferences based on the communication context, including when, where, and under what circumstances an interaction takes place.

Interactions of Two or More People

Social eavesdropping, by nature, occurs within communication networks, defined as "the patterns of contact between communication partners created by the flow of messages among communicators through time and space" (Monge & Contractor, 2003, p. 3). For social eavesdropping to occur, there must be at least three people involved: two or more interactants and an eavesdropper. This network-based perspective extends beyond humans. Animal communication scholars who study social eavesdropping use communication networks to model relationships beyond dyads, defining these networks as groups of several animals within signaling/receiving range of one another (Doutrelant & McGregor, 2000; Searcy & Nowicki, 2005).

Different types of ties exist in networks (Borgatti, Brass, & Halgin, 2014; Borgatti & Lopez-Kidwell, 2014), including similarities (e.g., participation in events, comemberships in groups, sharing attributes), social relations (e.g., kinship, role-based, perceptual, affective relationships), interactions (e.g., transactions and exchanges such as talking with or sending e-mail to) and flows (e.g., the movement of information, knowledge, goods, or other resources from one source to another). Our definition of social eavesdropping assumes that interaction ties among communicators provide opportunities for third parties to create social eavesdropping ties.

This network conceptualization eliminates the possibility of gathering information from the actions of one individual (e.g., observation; see Miller & Jablin, 1991). Information flows between the two interactants and from the interactants to the eavesdropper; it can also flow from the eavesdropper back to the interactants, influencing the eavesdropper's evaluation of social risk and information value. Social eavesdropping ties are asymmetric information flow ties (i.e., information flows from the interactants to the eavesdropper).

Using Goffman's (1979) terms, the interactants are "addressed" recipients and "ratified" participants in the conversation. Ratified participants negotiate privacy boundaries of information shared between them, but do not do so with the eavesdropper (Petronio, 2002, 2010).

Third-Party or Bystander

Not everyone who is listening to a conversation is an official participant. In fact, "a ratified participant may not be listening, and someone listening may not be a ratified participant" (Goffman, 1979, p. 8). The third person in the network who becomes a social eavesdropper is a bystander who is not the target audience (i.e., an unratified participant; see Goffman, 1979). The newly created social eavesdropping tie is an information flow tie in the network (Borgatti et al., 2014; Borgatti & Lopez-Kidwell, 2014).

The presence of social eavesdroppers can change how information flows in communication networks. In Figure 1, we depict hypothetical changes in the structures of information flow resulting from the presence of an eavesdropper.

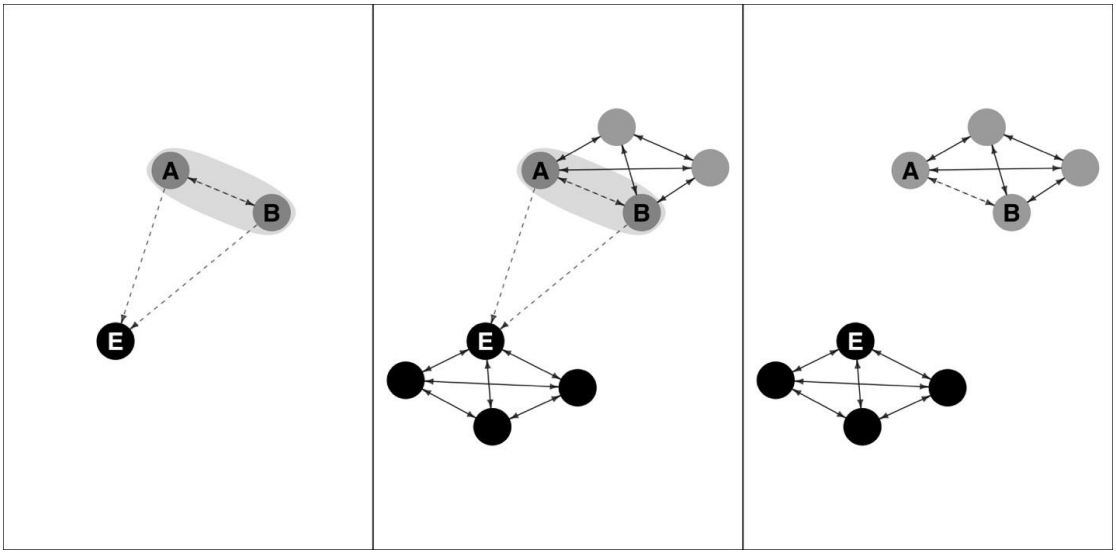

Figure 1. How eavesdropping affects information flow in communication networks.

A simple example of social eavesdropping network relations and dynamics is illustrated in Figure 1. The first panel illustrates the simplest social eavesdropping network isolated from the rest of the network. The interactants (A and B) exchange information, while the eavesdropper (E) obtains information from this interaction. The shadow highlighting A and B indicates their coordinated privacy boundary.

In the second panel, social eavesdropping is embedded in the larger network. Two groups are isolated from one another except for the information flow tie from the interactants to the eavesdropper. The within-group social relation ties, indicated by the solid lines with reciprocal arrows, can represent friendship groups, work teams, or any other sets of individuals of interest. Within these groups, private information is shared and managed through boundary coordination (Petronio, 2002, 2010). Privacy boundaries may not be coordinated at all between the interactants and the eavesdropper. If boundaries have been negotiated between the eavesdropper and interactants, boundary turbulence (i.e., some violation or misunderstanding of those boundaries) leads to a breach in presumably private information. Petronio (2002) gives the example of a person who overhears private information from a stranger on an airplane. In this case, "[the] person is not the intended target and therefore [has] less of an obligation to negotiate privacy rules for management" (p. 29).

Eavesdroppers embedded in different social groups than the interactants, as illustrated in the second panel, can transfer information to an entirely different group in a network with which boundary coordination has not occurred. In other words, eavesdroppers could provide gateways or bridges for those within one social group to get information about another social group with differential characteristics. This illustration embeds the eavesdropper and interactants in two different groups to illustrate how social eavesdropping may influence outcomes at higher levels of analysis. People may also eavesdrop on others in their same social group.

The third panel shows two isolated groups of individuals, meaning information is assumed to be exchanged within the group, but no known information is exchanged between groups. The eavesdropper is not shown to have access to the information shared between A and B or exchanged among A and B's group (i.e., E is not shown to be gathering information outside of their group).

Conceptualizing social eavesdropping as a communication network raises several research questions. From an information flow perspective, for example, we may ask how does the presence of one or more eavesdroppers change outcomes for an entire group or community? How are social eavesdropping ties formed? What makes it more likely for individuals to create social eavesdropping ties in a network? To uncover this, we focus on potential eavesdroppers as egos in egocentric networks by exploring the factors that influence whether people create eavesdropping ties in a network. In the following section, we present a conceptual model to examine the psychological and environmental factors that influence the likelihood of social eavesdropping.

Social Eavesdropping Conceptual Model

Our conceptual model, illustrated in Figure 2, draws on information gathering, signaling, and uncertainty management theories to understand whether an individual will create a social eavesdropping tie. This model includes three factors that influence the likelihood of an individual to eavesdrop: accessibility, information value, and social risk.

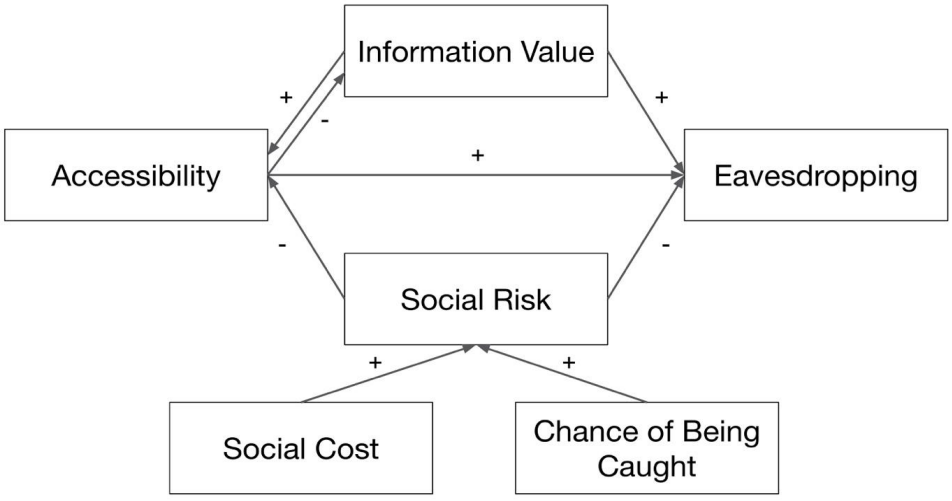

Figure 2. Conceptual model of social eavesdropping.

We explain each of these concepts and the relations between them in subsequent sections.

Accessibility

Social eavesdropping is only possible when the interactions of two or more people are accessible. In our model, accessibility is defined as "the level of difficulty associated with retrieving and interpreting the information" (Stohl, Stohl, & Leonardi, 2016, p. 129) in online and off-line environments. Accessibility is crucial for diverse information-seeking and gathering behavior (Borgatti & Cross, 2003; Choo, 2001; Monge & Contractor, 2003). For both passive and active social eavesdropping, there must be some minimum threshold of accessibility. If accessibility does not reach the threshold, social eavesdropping is not possible. For example, although many would love to eavesdrop on the interactions inside the U.S. presidential Oval Office, the minimum necessary level of accessibility to those interactions cannot be attained except by select individuals on the president's staff. Online screening criteria for a social media group may preclude someone from gaining access to interactions within that digital space. For instance, employees who want access to their boss's private Slack channel for company managers would be excluded for not fitting the criteria to join the channel.

If accessibility exceeds the necessary minimum threshold, social eavesdropping is possible, although not guaranteed. In off-line contexts, eavesdroppers must be close enough to detect and observe an interaction. In online or mediated contexts, interactions must be detectable and visible to eavesdroppers either in real time or as recorded digital traces (e.g., e-mails, online social forums such as chat rooms, blogs, or social media) through the affordances (i.e., limitations or possibilities of specific behaviors realized through relationships between people and material things) of visibility and persistence (Treem & Leonardi, 2013). Higher accessibility, whether obtained actively or passively, is therefore related to the likelihood of social eavesdropping all else being equal.

Proposition 1: As level of accessibility increases (given that accessibility exceeds the minimum threshold), the likelihood of social eavesdropping increases.

Accessibility is influenced by many environmental, network, and individual-level factors. Some factors that affect accessibility may be impossible (or very difficult) for potential eavesdroppers to change (e.g., a lone low-level employee cannot easily change an open office environment). However, individuals can control and alter some barriers to accessibility (e.g., moving closer to a cubicle where coworkers are conversing).

An often-immutable environmental factor, architecture influences privacy boundaries set by both physical (e.g., buildings with rooms, cubicles, or open workstations) and virtual design (e.g., Facebook privacy settings that restrict viewing user activity to the owner, owner's friends, or users worldwide). For example, open architecture environments may increase an individual's ability to both eavesdrop and be eavesdropped on by others (Archea, 1977). Research in organizational settings has indicated that when people move to open-plan workspaces, they miss the privacy that a walled office provides (Hedge, 1982; Oldham, 1988; Sundstrom, Herbert, & Brown, 1982). On the other hand, in a hospital environment, a central nurses' station provided space for information transfer in an open environment, thus facilitating eavesdropping (Vuckovic, Lavelle, & Gorman, 2004). Locke (2010) emphasizes that people in close proximity and open environments can observe behavioral information such as expressions, voice intonations, and eye gaze and more easily intercept whispers.

Just as physical barriers impact behavior in off-line spaces, architectural elements of online spaces such as passwords, permissions, and perceptions of "space" shape online behavior (Lessig, 2007). According to Lessig (2007), online space and structure help dictate the types of behaviors that are possible and also encourage or discourage certain relationships. A unique aspect of information flow online in comparison to off-line is that, depending on the design of the online space, communication traces may be persistent or fleeting (Treem & Leonardi, 2013). Eavesdroppers may obtain access to interactions that took place months ago in online spaces, such as conversation threads between people exchanging messages on Facebook.

Network structures also affect accessibility. Propinquity, or physical closeness, has been examined in network literature as a key factor influencing contact among social entities (e.g., Rivera, Soderstrom, & Uzzi, 2010). Physical closeness means more accessibility, which means a higher likelihood of creating eavesdropping ties. Changing physical proximity may be easy for some eavesdroppers (e.g., taking a break at the same time as others; see Reagans, 2010), but difficult for others (e.g., working in a different region). Network distance (i.e., the fewest number of ties between one entity to another) also plays a role in accessibility. The conversations of a friend of a friend are closer in the network and more accessible than those among individuals three or more hops away. Individual factors that affect accessibility, such as ability and time, are also important to consider in empirical work.

Once the threshold level of accessibility is reached, the perceptions of information value and social risk also influence the likelihood of social eavesdropping.

Information Value

Perceived information value is defined as a potential eavesdropper's perception of the utility of information that could be gained by creating a social eavesdropping tie. This can be distinguished from actual information value, which may or may not correspond to the perception of value. Perceived information value is high when a potential eavesdropper believes others have relevant and beneficial information that he or she lacks to fulfill a goal or desired state, broadly ranging from entertainment to functional needs (Case & Given, 2016; Stephenson, 1964). In other words, perceived information value is the motivating mechanism—people seek out (active) or encounter (passive) new and often useful information.

One main motivator to seek information is uncertainty or the unpredictability of an outcome. Uncertainty is spurred by situations perceived as ambiguous or complex, especially when information is inconsistent or unavailable (Berger, 2002; Bradac, 2001). According to uncertainty reduction theory, individuals are motivated to reduce their uncertainty by gathering information to make predictions about themselves, their environment, and the behavior of others (Berger & Calabrese, 1975). However, there may also be different "levels of motivation to reduce uncertainty" (Kramer, 1999, p. 306) depending on individual factors like tolerance for uncertainty. Uncertainty management approaches take this a step further by proposing that individuals may not always want to reduce uncertainty, and in some cases, individuals want to increase their perceived level of uncertainty (Brashers, 2001; Hogg & Belavadi, 2017). Uncertainty is appraised before taking any communicative action and can represent danger (i.e., not having the information leads to negative feelings like distress) or opportunity (i.e., not having the information leads to positive feelings like optimism; Brashers et al., 2000). In our model, the perceived value of information

gained by social eavesdropping is high in the former case (uncertainty = danger, so reducing uncertainty by gathering information would be positive) and low in the latter (uncertainty = opportunity, so reducing uncertainty by gathering information would be negative).

Perceived information value and uncertainty management are elements of information gathering generally, not just social eavesdropping. The question is, why would someone eavesdrop as opposed to gather information using one of myriad other ways, such as directly asking? Although Afifi and Weiner (2004) propose that "interrogating the target" (p. 182) may be the most efficient information-seeking method, we contend that this is not always the case. In fact, sometimes passive or indirect information-seeking is better suited for certain situations (Kramer, 2010; Miller & Jablin, 1991). When seeking information with the goal to reduce uncertainty, it is crucial that the information is honest and reliable. For example, people present themselves differently depending on where they are and with whom they are talking. Eavesdroppers may receive completely different information than what they would if they were gathering information directly. Not being the designated target audience may, in fact, be the reason why someone eavesdrops instead of gathering information in other ways (Goffman, 1979).

Signaling theory provides a lens to understand this behavior. In signaling theory, senders direct signals to receivers who rely on gathering honest information from hard-to-fake, more reliable signals to make better decisions (Connelly, Certo, Ireland, & Reutzel, 2010; Lewis, 2002; Skyrms, 2010). In some cases, receivers may not directly receive reliable, unmanipulated signals because information carriers often have incentives to keep information private (Stiglitz, 2002, pp. 463–464) or lie (Toma & Hancock, 2012). This can result in tension between information seekers and information carriers. A supervisor, for example, may hide knowledge about an upcoming layoff from their subordinates to forestall interpersonal conflict and decreased productivity. Of course, subordinates would prefer knowing this in advance, but may only be able to learn about it by eavesdropping on conversations among superiors.

In the case of social eavesdropping, the sender does not direct their communication to the eavesdropper, so they may be less likely (or perceived less likely by the eavesdropper) to manipulate signals that disadvantage the eavesdropper (Goffman, 1979). For instance, someone may eavesdrop on a conversation in which they are aware that one or more interactants are lying. Social eavesdropping on this interaction provides layers of information beyond the message itself. It provides information about the individuals telling the lie (e.g., untrustworthy) and those being lied to (e.g., gullible), as well as the relationship between the interactants (e.g., tenuous, tense, imbalanced). In this situation, the eavesdropper now has a considerable amount of leverage over the interactants.

Additionally, certain information is not readily available through conventional information-seeking strategies such as directly asking the target, a common strategy explored in the uncertainty management literature (Berger, 2002; Hogg & Belavadi, 2017). For example, directly asking about a new supervisor's leadership style may provide less accurate and complete information compared with eavesdropping on interactions between the supervisor and subordinates. Instead, indirect information-seeking tactics can provide an unobtrusive method to gather such information (Miller & Jablin, 1991). Social eavesdropping is an information-gathering method that can afford access to unfiltered information that people crave (Locke, 2010).

Perceptions of the network may also influence perceived information value. People make evaluations and decisions based on the cognitive representation of patterns of connections around them (Brands, 2013; Krackhardt, 1987). Eavesdroppers perceive their position in the network relative to the interactants. That position may influence their evaluations of the value of interactants' information (e.g., the eavesdropper occupies a bridge between their social group and the interactants'; see Figure 1, Panel 2). Eavesdroppers' perception of interactants' network positions, either between each other or as a pair/group in relation to the whole network, may also change their evaluations of information value.

Additionally, potential eavesdroppers who suspect information may flow from them back to the interactants (i.e., the interactants are aware of the eavesdropper and/or the eavesdropper reacts to the information gathered) because of their physical or network position may reevaluate and question the reliability of the information or whether the interactants are acting performatively/manipulatively because of their presence. As such, perceived network relations also play a role in perceived information value.

In the case of passive social eavesdropping, information is initially accessible. Perceived information value increases the likelihood of social eavesdropping, all else being equal. For example, a professor's ears perk up at a conference when she hears a nearby group of young academics discussing her most recently published book.

Proposition 2(a): As perceived information value increases, the likelihood of social eavesdropping increases.

An eavesdropper's perception of information value is affected by various factors, including accessibility. In a workplace, for example, if a supervisor closes her office door to have a discussion, those on the other side of the closed door will perceive that information as being more valuable because it is private. Scarcity enhances the value or desirability of information (Lynn, 1991). Scarce information, by definition, is less accessible, which influences perceived information value related to fulfilling a desired goal or state.

Proposition 2(b): As accessibility decreases, perceived information value increases.

At any given time, many interactions may be accessible to a potential eavesdropper. Based on scarcity logic, they view less accessible information as more valuable to gather. In this case, the potential eavesdroppers will try to increase their accessibility, leading to active social eavesdropping at a later point in time. Alternatively, if they do not perceive the information as being valuable (Brashers et al., 2000), the potential eavesdroppers may decrease their accessibility, resulting in no social eavesdropping.

Proposition 2(c): As perceived information value increases, individuals are more likely to increase their accessibility to engage in active social eavesdropping.

Though perceived information value is a motivating mechanism for social eavesdropping, costs and social risks are deterrents.

Costs and Social Risks

Social eavesdropping has inherent costs, defined as the loss of something of value to an individual. These costs may be either actual or anticipated. Actual costs occur by the act of social eavesdropping (e.g., time, effort), and vary based on whether social eavesdropping is passive or active.

Anticipated costs are costs that individuals believe will be imposed because of social eavesdropping. These anticipated costs may be related to the type of information gathered (e.g., learning negative information can be costly); these costs also include any other expected loss of something of value after and because of social eavesdropping. For example, there may be anticipated costs associated with lost attention on other matters.

Social costs are a particularly relevant type of anticipated costs for social eavesdropping. Miller and Jablin (1991) relate social costs to "receiving the obverse of social rewards (e.g., social rejection instead of social approval)" (p. 95) in the context of social exchange. Taking this relational perspective, we define social costs as negative consequences administered by others. Any process of gathering information involves varying degrees of anticipated embarrassment, punishment via social sanctions, loss of face, and damaged relationships (Cooper-Thomas & Stadler, 2015; Hsieh, 2009; Morrison & Vancouver, 2000). Hsieh (2009) found organizational members were more likely to use covert tactics such as surveillance rather than asking their boss directly, for example, because direct asking posed higher social risks (e.g., looking incompetent). Social eavesdropping may be especially prone to social cost concerns because the behavior has been historically stigmatized and has ties to privacy and ethical concerns (Locke, 2010).

For those negative consequences to be administered, an eavesdropper must be identified by others. Perceived social risk, then, is a function of (1) the perceived severity of social consequences or costs and (2) the perceived chance of being caught (Deline & Kahlor, 2019; Kasperson et al., 1988). The concept of "getting caught" is unique to social eavesdropping as an information-gathering method. It is also a factor in decision-making models related to illicit activities like purchasing illegal goods (Albers-Miller, 1999). The perceived chance of getting caught influences the perceived certainty of receiving social costs (Hollinger & Clark, 1983). Social costs will be administered only if caught (i.e., it is a necessary, but not sufficient condition). Many information-gathering methods are overt, so individuals are not concerned about getting caught. Even covert methods or indirect information-gathering methods are often encouraged (e.g., observing and monitoring; Miller & Jablin, 1991).

Social eavesdropping is often covert, particularly in situations where it is socially costly. To explore how the perceived chance of being caught affects the likelihood of social eavesdropping, the relative weights of various factors must be considered. For instance, the information value must be very high, and the perceived chances of getting caught must be very low for an individual to eavesdrop in high-cost situations. Individual factors related to risk, like risk-aversion or risk tolerance (Tan & Zhao, 2003), also may affect the relative likelihood of social eavesdropping.

For example, a low-level employee whose anticipated cost of social eavesdropping is losing his job may still eavesdrop if the information is highly valuable (e.g., it could benefit career mobility), if the expected

chances of being discovered are fairly low (e.g., eavesdropping on the C-suite executives of a large company at a coffee shop with back to interactants), and/or if the individual is risk tolerant such that anticipated social costs do not factor as heavily in the decision to eavesdrop. How each individual weighs the different factors will depend on individual and environmental characteristics. In general, however, higher perceived social risk (as a function of anticipated social costs and perceived chance of being caught) results in a lower likelihood of social eavesdropping, all else being equal.

Proposition 3: As perceived social risk increases, the likelihood of social eavesdropping decreases.

Like information value, perceived social risk influences how potential eavesdroppers may change their accessibility to avoid social eavesdropping or engage in active social eavesdropping. If perceived social risk is high, potential eavesdroppers are more likely to decrease their current accessibility; if perceived social risk is low, potential eavesdroppers are more likely to increase their accessibility because potential harm is low.

Proposition 4: As perceived social risk increases, individuals are more likely to lower their accessibility to avoid social eavesdropping.

Proposition 5: As perceived social risk decreases, individuals are more likely to increase their accessibility to engage in active social eavesdropping.

Evaluations of social risk are also influenced by perceived network position. For example, believing one is in a particularly vulnerable network position (e.g., could be excluded from a large portion of the network if he or she were cut off by one or two individuals), the individual may perceive greater social risk. If potential eavesdroppers believe information would flow from them to the interactants, they may evaluate greater social risk compared with whether they believed the information flow tie would not exist (e.g., they are covert).

Discussion

Our model considers social eavesdropping from the perspective of the eavesdropper. The potential eavesdropper evaluates information value and social risk while situated in a high or low accessibility environment. On reaching satisfactory levels of accessibility, individuals will socially eavesdrop either passively or actively to obtain information. While the model appears simple, the dynamic interplay among factors makes social eavesdropping behavior and outcomes intriguing topics of study.

Additionally, this conceptualization helps clarify how social eavesdropping is similar to and different from related terms such as surveillance, lurking, ambient awareness, and other covert or unobtrusive information-gathering tactics. As surveillance has been previously defined as "any collecting or processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been gathered" (Lyon, 2001, p. 2), some social eavesdropping can be considered as a form of surveillance. By this definition, surveillance is distinguished from social eavesdropping in that it encompasses a broader range of information-collecting strategies and behavior with the explicit purpose of

managing and influencing others. Surveillance includes situations in which data are collected on individuals who are not interacting with others. Therefore, there is an overlapping yet distinct relation between surveillance and social eavesdropping.

Lurkers are people who only observe and rarely or never post in online communities (Preece, Nonnecke, & Andrews, 2004). Lurking, like social eavesdropping, can be both normal and valuable—used to learn about group norms and gain knowledge from others (Edelmann, 2013; Sun, Rau, & Ma, 2014). To distinguish when lurking may be a type of social eavesdropping, we must consider how situation and context influence the enactment of privacy rules (Petronio, 2002). Online spaces are unique in that collective privacy boundaries are established with those engaging on the site (Child & Starcher, 2016). However, there may be both known and unknown individuals accessing content. As former U.S. Secretary of Defense Donald Rumsfeld once said, "There are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know" (Graham, 2014, para. 2). By the definition established in this work, only "unknown" unknown lurkers would be eavesdroppers because of privacy boundary turbulence; "known" unknown lurkers would be part of implied boundary coordination and given permission to access posted information on blogs or social media (Child & Starcher, 2016).

Ambient awareness occurs when a third party perceives others' communication as "merely background noise" but the awareness results in productive changes in their knowledge and outcomes (Leonardi & Meyer, 2014, p. 18). Ambient awareness is not an active communicative behavior, but rather something that happens when environmental conditions are conducive. Leonardi and Meyer (2014) focus on how social networking sites can facilitate ambient awareness by making "the bits and pieces of information communicated by others throughout time" visible (p. 18). Social eavesdropping, on the other hand, occurs either serendipitously or actively and can happen in both online and off-line spaces. Although some cases of ambient awareness may be classified as serendipitous or passive social eavesdropping, our conceptualization both extends and further disentangles the factors that influence this behavior.

Scope and Future Directions

Our model's scope is bounded with social eavesdropping as the outcome. Once social eavesdropping has occurred, however, the gathered information may have unique qualities compared with information gathered using more direct methods. Perhaps information gathered through social eavesdropping is more inherently costly to know. On the other hand, social eavesdropping may result in a "second-order" information asymmetry in which the interactants do not presently know that the eavesdropper knows what they know.[3] Theorizing the nature of the information gained and how that information is used by the eavesdropper would further distinguish social eavesdropping from other, more transparent methods of information gathering.

[3] The caveat is that eavesdroppers may receive noisy information with inaccuracies because of the nature of gathering (e.g., being far away, misunderstanding context, only hearing parts of a conversation).

The interactants' perspectives of social eavesdropping must also be explored. If the interactants view their information as private, they believe that they own this information, and they should control who has access to it (Petronio, 2002). Expectations of privacy exist on a continuum depending, among other things, on the environment (see Petronio, 2010, p. 182)—specifically, whether it is a very porous informational environment (e.g., a more-public company break room) or a solid, nonporous informational environment (e.g., a private office). Interactants may also engage in highly manipulative behavior to distract, intentionally mislead, or lure potential eavesdroppers. For example, if interactants realize that an eavesdropper is present, they may create informational barriers or change the messages they send (e.g., speak in a different language so that others in the room cannot understand) to avoid transferring information to an unratified participant in the conversation. In contrast, another example may involve interactants who want to transfer information, but also want the eavesdropper to believe that this information is unfiltered, not directed at them, and therefore more reliable.

Scholars must also theorize about the consequences of social eavesdropping. In other words, social eavesdropping may be an input or predictor rather than the outcome. Sometimes, information asymmetries between different parties may change without the knowledge of all actors in the network, especially if covert social eavesdropping causes the change in asymmetry. For example, if an eavesdropper learns unexpected negative information, would this change their future behavior? Under what conditions would social eavesdropping result in conflict as opposed to positive outcomes? Could social eavesdropping at one time lead to more in the future? Could high social risk environments deter future social eavesdropping and change the information flow more broadly? Future work should address these questions in detail.

Empirical studies can investigate how social eavesdropping poses differential effects on individuals, groups, organizations, and other stakeholders. For example, previous research in organizational behavior and communication indicates that information seeking is critical to reducing job uncertainty, particularly for newcomers (Miller & Jablin, 1991; Morrison, 2002). Social eavesdropping may be more beneficial than other information-seeking tactics, especially when it would be costly for interactants to turn their attention away from their job to address a third party, such as the case of the nurses eavesdropping on doctors in the cardiac intensive care unit (Vuckovic et al., 2004). The prevalence of social eavesdropping must also be determined; how often does social eavesdropping occur, particularly passive compared with active? We suspect passive social eavesdropping occurs more often, though active may result in more interesting positive and negative outcomes.

Sometimes online and off-line contexts may collide as individuals reveal their social eavesdropping experiences from one context to another. As illustrated by the opening Twitter example, people may eavesdrop in off-line environments and share the information gained in online contexts to spread it more widely. There is also evidence that people perceive deception differently in mediated and face-to-face contexts (Toma & Hancock, 2012), suggesting that social eavesdropping could be a way for people to mitigate perceived (though not necessarily actual) deception.

Additionally, widely available mobile video, electronic surveillance, and wiretapping technologies give individuals, organizations, and governments the capability to record and distribute unparalleled levels of personal and social information (Marwick, 2012). Once the decision is made to eavesdrop, the

eavesdropper also decides whether to record and/or share information (Hagen, Bighash, Hollingshead, Shaikh, & Alexander, 2018). Social media greatly expands the potential number of second-hand social eavesdroppers, people who gain access to surreptitiously recorded conversations and events through social sharing. This can have dramatic and far-reaching consequences that transcend the triadic relationships explored here and deserve future research attention.

The influence of social eavesdropping on the behaviors of those being monitored should also be explored. Keeping information private in the digital age is difficult; people often must make concerted efforts to adjust settings online such as "opting out" (Bimber, Flanagin, & Stohl, 2005). Boundaries between private and public space become increasingly blurred as technologies like mobile phones (Katz & Aakhus, 2002) and social media sites (McDonald & Thompson, 2016) make serendipitous encounters more common. The visibility of communication along with the presence or absence of a suspected eavesdropper online may affect how interactants behave in the first place, influencing the information that may be gathered by eavesdroppers (Treem, Leonardi, & van den Hooff, 2020). Future work should also address how the presence of eavesdroppers may change privacy management through evaluations and negotiations of boundary permeability, ownership, control, linkages, and turbulence (Mills et al., 2012; Petronio, 2002, 2010).

Conclusion

Developing a theoretical model of social eavesdropping is critical at this time for three reasons. First, although many scholars have developed useful models of information gathering and uncertainty management, social eavesdropping itself has not been explicated from a social science perspective. Second, social network analysis is becoming more common and useful in communication research. Including social eavesdropping ties in network analyses may provide additional insight into the nature of information flow and network outcomes like virality. Finally, new technologies allow people to eavesdrop in new ways never before imagined. No longer are we only confined to eavesdropping in the physical presence of others. Whether one peers into the personal conversation of others in messages on social media or uses technology to listen in on a conversation far away, these behaviors are now possible because of technology. The systematic model developed here applies to both off-line (either aided by technology or not) and online environments and will assist researchers wishing to explore this unique method of information gathering.

References

Afifi, W. A., & Weiner, J. L. (2004). Toward a theory of motivated information management. *Communication Theory*, *14*(2), 167–190. doi:10.1111/j.1468-2885.2004.tb00310.x

Albers-Miller, N. D. (1999). Consumer misbehavior: Why people buy illicit goods. *Journal of Consumer Marketing*, *16*(3), 273–287. doi:10.1108/07363769910271504

Anderson, M. H. (2008). Social networks and the cognitive motivation to realize network opportunities: A study of managers' information gathering behaviors. *Journal of Organizational Behavior*, *29*(1), 51–78. doi:10.1002/job.459

Archea, J. (1977). The place of architectural factors in behavioral theories of privacy. *Journal of Social Issues*, *33*(3), 116–137. doi:10.1111/j.1540-4560.1977.tb01886.x

Bates, M. J. (2002). Toward an integrated model of information seeking and searching. *New Review of Information Behaviour Research*, *3*(1), 1–15. Retrieved from https://pages.gseis.ucla.edu/faculty/bates/articles/info_SeekSearch-i-030329.html

Berger, C. R. (2002). Strategic and nonstrategic information acquisition. *Human Communication Research*, *28*(2), 287–297. doi:10.1111/j.1468-2958.2002.tb00809.x

Berger, C. R., & Calabrese, R. J. (1975). Some explorations in initial interaction and beyond: Toward a developmental theory of interpersonal communication. *Human Communication Research*, *1*(2), 99–112. doi:10.1111/j.1468-2958.1975.tb00258.x

Bimber, B., Flanagin, A. J., & Stohl, C. (2005). Reconceptualizing collective action in the contemporary media environment. *Communication Theory*, *15*(4), 365–388. doi:10.1111/j.1468-2885.2005.tb00340.x

BliegeBird, R., Smith, E., Alvard, M., Chibnik, M., Cronk, L., Giordani, L., . . . Bird, R. (2005). Signaling theory, strategic interaction, and symbolic capital. *Current Anthropology*, *46*(2), 221–248. doi:10.1086/427115

Borgatti, S. P., Brass, D. J., & Halgin, D. S. (2014). Social network research: Confusions, criticisms, and controversies. In D. J. Brass, G. Labianca, A. Mehra, D. S. Halgin, & S. P. Borgatti (Eds.), *Contemporary perspectives on organizational social networks* (Vol. 40, pp. 1–29). Bingley, UK: Emerald.

Borgatti, S. P., & Cross, R. (2003). A relational view of information seeking and learning in social networks. *Management Science*, *49*(4), 432–445. doi:10.1287/mnsc.49.4.432.14428

Borgatti, S. P., & Lopez-Kidwell, V. (2014). Network theory. In J. Scott & P. J. Carrington (Eds.), *The SAGE handbook of social network analysis* (pp. 40–54). London, UK: SAGE Publications.

Bradac, J. J. (2001). Theory comparison: Uncertainty reduction, problematic integration, uncertainty management, and other curious constructs. *Journal of Communication*, *51*(3), 456–476. doi:10.1111/j.1460-2466.2001.tb02891.x

Brands, R. A. (2013). Cognitive social structures in social network research: A review. *Journal of Organizational Behavior*, *34*(S1), S82–S103. doi:10.1002/job.1890

Brashers, D. E. (2001). Communication and uncertainty management. *Journal of Communication*, *51*(3), 477–497. doi:10.1111/j.1460-2466.2001.tb02892.x

Brashers, D. E., Neidig, J. L., Haas, S. M., Dobbs, L. K., Cardillo, L. W., & Russell, J. A. (2000). Communication in the management of uncertainty: The case of persons living with HIV or AIDS. *Communication Monographs*, *67*(1), 63–84. doi:10.1080/03637750009376495

Case, D. O., & Given, L. M. (2016). *Looking for information: A survey of research on information seeking, needs, and behavior* (4th ed.). Bingley, UK: Emerald.

Cheney, D. L., & Seyfarth, R. M. (2005). Social complexity and the information acquired during eavesdropping by primates and other animals. In P. K. McGregor (Ed.), *Animal communication networks* (pp. 583–604). Cambridge, UK: Cambridge University Press.

Child, J. T., & Starcher, S. C. (2016). Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management. *Computers in Human Behavior*, *54*, 483–490. doi:10.1016/j.chb.2015.08.035

Choo, C. W. (2001). Environmental scanning as information seeking and organizational learning. *Information Research*, *7*(1), 7–1. Retrieved from http://informationr.net/ir/7-1/paper112.html

Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2010). Signaling theory: A review and assessment. *Journal of Management*, *37*(1), 39–67. doi:10.1177/0149206310388419

Cooper-Thomas, H. D., & Stadler, M. J. (2015). Costs and benefits of newcomer adjustment tactics. *International Journal of Selection and Assessment*, *23*(2), 160–173. doi:10.1111/ijsa.12104

Deline, M. B., & Kahlor, L. A. (2019). Planned risk information avoidance: A proposed theoretical model. *Communication Theory*, *29*(3), 360–382. doi:10.1093/ct/qty035

Donath, J. (2007). Signals in social supernets. *Journal of Computer-Mediated Communication*, *13*(1), 231–251. doi:10.1111/j.1083-6101.2007.00394.x

Doutrelant, C., & McGregor, P. K. (2000). Eavesdropping and mate choice in female fishing fish. *Behaviour*, *137*(12), 1655–1668. doi:10.1163/156853900502763

Eavesdrop. (n.d.). In *Merriam-Webster's online dictionary*. Retrieved from https://www.merriam-webster.com/dictionary/eavesdropper

Edelmann, N. (2013). Reviewing the definitions of "lurkers" and some implications for online research. *Cyberpsychology, Behavior, and Social Networking*, *16*(9), 645–649. doi:10.1089/cyber.2012.0362

Goffman, E. (1979). Footing. *Semiotica*, *25*(1), 1–30. doi:10.1515/semi.1979.25.1-2.1

Graham, D. A. (2014, March 27). Rumsfeld's knowns and unknowns: The intellectual history of a quip. *The Atlantic*. Retrieved from https://www.theatlantic.com/politics/archive/2014/03/rumsfelds-knowns-and-unknowns-the-intellectual-history-of-a-quip/359719/

Hagen, C. S., Bighash, L., Hollingshead, A. B., Shaikh, S. J., & Alexander, K. S. (2018). Why are you watching? Video surveillance in organizations. *Corporate Communications: An International Journal*. doi:10.1108/CCIJ-04-2017-0043

Hedge, A. (1982). The open-plan office: A systematic investigation of employee reactions to their work environment. *Environment and Behavior*, *14*(5), 519–542. doi:10.1177/0013916582145002

Hogg, M. A., & Belavadi, S. (2017). Uncertainty management theories. In M. A. Hogg & S. Belavadi (Eds.), *Oxford research encyclopedia of communication*. Oxford, UK: Oxford University Press. doi:10.1093/acrefore/9780190228613.013.495

Hollinger, R. C., & Clark, J. P. (1983). Deterrence in the workplace: Perceived certainty, perceived severity, and employee theft. *Social Forces*, *62*(2), 398–418. doi:10.1093/sf/62.2.398

Hsieh, M. H. (2009). Human centric knowledge seeking strategies: A stakeholder perspective. *Journal of Knowledge Management*, *13*(4), 115–133. doi:10.1108/13673270910971879

Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R., . . . Ratick, S. (1988). The social amplification of risk: A conceptual framework. *Risk Analysis*, *8*(2), 177–187. doi:10.1111/j.1539-6924.1988.tb01168.x

Katz, J. E., & Aakhus, M. (Eds.). (2002). *Perpetual contact: Mobile communication, private talk, public performance*. New York, NY: Cambridge University Press.

Kellermann, K. (1992). Communication: Inherently strategic and primarily automatic. *Communication Monographs*, *59*(3), 288–300. doi:10.1080/03637759209376270

Krackhardt, D. (1987). Cognitive social structures. *Social Networks*, *9*(2), 109–134. doi:10.1016/0378-8733(87)90009-8

Kramer, M. W. (1999). Motivation to reduce uncertainty: A reconceptualization of uncertainty reduction theory. *Management Communication Quarterly*, *13*(2), 305–316. doi:10.1177/0893318999132007

Kramer, M. W. (2010). *Organizational socialization: Joining and leaving organizations*. Malden, MA: Polity Press.

LeggyBald. (2019, July 5). What's the strangest conversation you've "accidentally" eavesdropped on? [Online forum post]. Retrieved from https://www.reddit.com/r/AskReddit/comments/c9hhgh/whats_the_strangest_conversation_youve/

Leonardi, P. M., & Meyer, S. R. (2014). Social media as social lubricant: How ambient awareness eases knowledge transfer. *American Behavioral Scientist*, *59*(1), 10–34. doi:10.1177/0002764214540509

Lessig, L. (2007). *Code: Version 2.0*. New York, NY: Basic Books.

Lewis, D. (2002). *Convention: A philosophical study*. Oxford, UK: Blackwell.

Locke, J. L. (2005). Looking for, looking at: Social control, honest signals, and intimate experience in human evolution and history. In P. K. McGregor (Ed.), *Animal communication networks* (pp. 416–441). Cambridge, UK: Cambridge University Press.

Locke, J. L. (2010). *Eavesdropping: An intimate history*. Oxford, UK: Oxford University Press.

Lynn, M. (1991). Scarcity effects on value: A quantitative review of the commodity theory literature. *Psychology & Marketing*, *8*(1), 43–57. doi:10.1002/mar.4220080105

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Buckingham, UK: Open University Press.

Magrath, R. D., Haff, T. M., Fallow, P. M., & Radford, A. N. (2015). Eavesdropping on heterospecific alarm calls: From mechanisms to consequences. *Biological Reviews*, *90*(2), 560–586. doi:10.1111/brv.12122

Marwick, A. (2012). The public domain: Surveillance in everyday life. *Surveillance & Society*, *9*(4), 378–393. doi:10.24908/ss.v9i4.4342

McDonald, P., & Thompson, P. (2016). Social media (tion) and the reshaping of public/private boundaries in employment relations. *International Journal of Management Reviews*, *18*(1), 69–84. doi:10.1111/ijmr.12061

Miller, V. D., & Jablin, F. M. (1991). Information seeking during organizational entry: Influences, tactics, and a model of the process. *Academy of Management Review*, *16*(1), 92–120. doi:10.5465/AMR.1991.4278997

Mills, C. M., Danovitch, J. H., Grant, M. G., & Elashi, F. B. (2012). Little pitchers use their big ears: Preschoolers solve problems by listening to others ask questions. *Child Development*, *83*(2), 568–580. doi:10.1111/j.1467-8624.2011.01725.x

Monge, P. R., & Contractor, N. S. (2003). *Theories of communication networks*. New York, NY: Oxford University Press.

Morrison, E. W. (1993). Newcomer information seeking: Exploring types, modes, sources, and outcomes. *Academy of Management Journal*, *36*(3), 557–589. doi:10.5465/256592

Morrison, E. W. (2002). Information seeking within organizations. *Human Communication Research*, *28*(2), 229–242. doi:10.1111/j.1468-2958.2002.tb00805.x

Morrison, E. W., & Vancouver, J. B. (2000). Within-person analysis of information seeking: The effects of perceived costs and benefits. *Journal of Management*, *26*(1), 119–137. doi:10.1177/014920630002600101

Oldham, G. R. (1988). Effects of changes in workspace partitions and spatial density on employee reactions: A quasi-experiment. *Journal of Applied Psychology*, *73*(2), 253–258. doi:10.1037/0021-9010.73.2.253

Peake, T. M. (2005). Eavesdropping in communication networks. In P. K. McGregor (Ed.), *Animal communication networks* (pp. 13–37). Cambridge, UK: Cambridge University Press.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany: State University of New York Press.

Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory & Review*, *2*(3), 175–196. doi:10.1111/j.1756-2589.2010.00052.x

Preece, J., Nonnecke, B., & Andrews, D. (2004). The top five reasons for lurking: Improving community experiences for everyone. *Computers in Human Behavior*, *20*(2), 201–223. doi:10.1016/j.chb.2003.10.015

Reagans, R. (2010). Close encounters: Analyzing how social similarity and propinquity contribute to strong network connections. *Organization Science*, *22*(4), 835–849. doi:10.1287/orsc.1100.0587

Rivera, M. T., Soderstrom, S. B., & Uzzi, B. (2010). Dynamics of dyads in social networks: Assortative, relational, and proximity mechanisms. *Annual Review of Sociology*, *36*(1), 91–115. doi:10.1146/annurev.soc.34.040507.134743

Romano, A. (2014, July 24). Coder livetweets sexist remarks allegedly made by IBM executives. *Daily Dot.* Retrieved from https://www.dailydot.com/debug/sexist-ibm-execs-overheard-at-lunch-in-tweets/

Savolainen, R. (2016). Elaborating the conceptual space of information-seeking phenomena. *Information Research*, *21*(3). Retrieved from http://InformationR.net/ir/21-3/paper720.html

Searcy, W., & Nowicki, S. (2005). *The evolution of animal communication: Reliability and deception in signaling systems*. Princeton, NJ: Princeton University Press.

Skyrms, B. (2010). *Signals: Evolution, learning, and information*. Oxford, UK: Oxford University Press.

Stephenson, W. (1964). *The play theory of mass communication*. New Brunswick, NJ: Transaction.

Stiglitz, J. E. (2002). Information and the change in the paradigm in economics. *American Economic Review*, *92*(3), 460–501. doi:10.1257/00028280260136363

Stohl, C., Stohl, M., & Leonardi, P. M. (2016). Managing opacity: Information visibility and the paradox of transparency in the digital age. *International Journal of Communication*, *10*, 123–137. Retrieved from http://ijoc.org/index.php/ijoc/article/view/4466

Sun, N., Rau, P. P.-L., & Ma, L. (2014). Understanding lurkers in online communities: A literature review. *Computers in Human Behavior*, *38*, 110–117. doi:10.1016/j.chb.2014.05.022

Sundstrom, E., Herbert, R. K., & Brown, D. W. (1982). Privacy and communication in an open-plan office: A case study. *Environment and Behavior*, *14*(3), 379–392. doi:10.1177/0013916582143007

Tan, H. H., & Zhao, B. (2003). Individual and perceived contextual-level antecedents of individual technical information inquiry in organizations. *The Journal of Psychology*, *137*(6), 597–621. doi:10.1080/00223980309600637

Toma, C. L., & Hancock, J. T. (2012). What lies beneath: The linguistic traces of deception in online dating profiles. *Journal of Communication*, *62*(1), 78–97. doi:10.1111/j.1460-2466.2011.01619.x

Treem, J. W., & Leonardi, P. M. (2013). Social media use in organizations: Exploring the affordances of visibility, editability, persistence, and association. *Annals of the International Communication Association*, *36*(1), 143–189. doi:10.1080/23808985.2013.11679130

Treem, J. W., Leonardi, P. M., & van den Hooff, B. (2020). Computer-mediated communication in the age of communication visibility. *Journal of Computer-Mediated Communication, 25*(1), 44–59. doi:10.1093/jcmc/zmz024

Varian, E. (2019, April 18). Overheard LA—The Instagram account that has L.A. talking (and eavesdropping). *Los Angeles Times*. Retrieved from https://www.latimes.com/home/la-hm-overheard-la-jesse-margolis-20190409-story.html

Vuckovic, N. H., Lavelle, M., & Gorman, P. (2004). Eavesdropping as normative behavior in a cardiac intensive care unit. *JHQ Online*, *5*, 1–6. Retrieved from https://www.researchgate.net/profile/Paul_Gorman6/publication/265191873_Eavesdropping_as_Normative_Behavior_in_a_Cardiac_Intensive_Care_Unit/links/54c262f00cf2911c7a4742e6.pdf

Weninger, T. (2014). An exploration of submissions and discussions in social news: Mining collective intelligence of Reddit. *Social Network Analysis and Mining*, *4*, 173. doi:10.1007/s13278-014-0173-9

Williams, L. (2014, July 24). Woman says she overheard IBM execs say they won't hire women because they get "pregnant again and again." *Think Progress.* Retrieved from https://archive.thinkprogress.org/woman-says-she-overheard-ibm-execs-say-they-wont-hire-women-because-they-get-pregnant-again-and-2df1329df53a/

Williamson, K. (1998). Discovered by chance: The role of incidental information acquisition in an ecological model of information use. *Library & Information Science Research*, *20*(1), 23–40. doi:10.1016/S0740-8188(98)90004-4