HUMAN-MACHINE COMMUNICATION

Human-Machine Communication
Volume 10, 2025
https://doi.org/10.30658/hmc.10.10

Creepy, Invasive, and Exploitative Algorithms: A CPM Analysis of Users' Privacy Breakdowns and Recalibration Practices With Social Media Algorithms

Matthew J. A. Craig[1] **and Jeffrey T. Child**[2]

1 COMBOTLABS-CMU, School of Communication, Journalism, and Media, Central Michigan University, Mount Pleasant, MI, USA
2 Department of Communication Studies, University of Nevada, Las Vegas, Las Vegas, NV, USA

Abstract

Social media content filtering algorithms can both provide desired personalized content and ads for users. However, sometimes these recommendations can resemble individual private information. How might users navigate these experiences to best manage their private information? The present exploratory study utilizes the rules- and systems-based framework of communication privacy management (CPM) theory to explore social media users' ($N = 636$) experiences of privacy breakdowns with social media algorithms and investigates what users do in response to said breakdowns. These responses were refined using content analysis and divided into different categories of privacy breakdowns and recalibration strategies. Implications for future research surrounding human-machine communication privacy management are discussed in light of our findings.

Keywords: human-centered computing, social media algorithms, communication privacy management, privacy turbulence, human-machine communication privacy management

CONTACT Matthew J. A. Craig • matthew.craig@cmich.edu • School of Communication, Journalism, and Media • Central Michigan University • Moore Hall 333 • Mount Pleasant, MI 48859

ISSN 2638-602X (print)/ISSN 2638-6038 (online)
www.hmcjournal.com

Introduction

Social media platforms leverage content-filtering algorithms for personalized user experiences (Auxier & Anderson, 2021). However, the opaque nature of these algorithms—the "black box" problem—can lead to user uncertainty about how and what data algorithms are used to provide recommendations. This lack of transparency often results in users forming folk theories or mental models to interpret unexpected or invasive algorithmic behaviors (e.g., DeVito et al., 2018). While personalization features can help cultivate a desired media feed, the algorithm's predictions about the user can sometimes be related to information they may not necessarily have wanted the algorithm to predict or know. Algorithmic transparency, or lack thereof, is critical because users frequently cannot verify how or why particular private information appears on their feeds. This opacity contributes significantly to privacy violations, as it fosters uncertainty, confusion, and discomfort among users, shaping their perceptions and responses. This study aims to understand better users' experiences of privacy breakdowns with social media algorithms and how they respond to them.

Exploration of the privacy management practices associated with social media algorithms is important, given that users like and dislike receiving curated content. For example, when users perceive an algorithm as sophisticated, they trust it more and are more comfortable sharing private information (Springer et al., 2017). However, users also dislike when search engines and websites track their search behaviors without their awareness to provide targeted advertising (Heimlich, 2012). Personalization can broadly be seen as helpful, creepy, or undesirable when recommendations are based too much on sensitive or private information (Dolin et al., 2018; Leon et al., 2013; Ur et al., 2012).

Social media users must ascribe social media algorithms some form of agency to cultivate a feed that meets their needs through content and recommended advertisements (Drüeke & Peil, 2024; Ellison et al., 2011; Taylor & Choi, 2024). Deciding what to recommend to users primarily involves the algorithm's logic and user input. Specifically, users engage in human-algorithm interplay by allowing algorithms to make certain recommendations by disclosing interests and using users' micro-bits of data scrubbed by the algorithm. While users may not directly disclose some of the private information utilized by algorithms, algorithms use all information available about a user to make ad recommendations (Diakopoulos, 2019; Eslami et al., 2015; Gillespie, 2014; Taylor & Choi, 2024).

When users encounter advertisements they cannot explain, they make assumptions about how the algorithm arrived at its recommendations (e.g., folk theories; DeVito et al., 2018; Lee et al., 2022). Based on users' micro-bits of collected data, these recommendations lead users to feel privacy turbulence because such predictions are too accurate and viewed by the individual as something the platform's algorithm should not know to recommend. CPM theory posits that individuals feel like they should have primary control over any information about them that is accessed, stored, or utilized by a machine agent (Petronio & Child, 2020). As such, individual social media users provide feedback to an algorithm on how it cultivates their feed. They do this by telling the algorithm what ads to never show again and by clicking on or sharing the ads they like. We refer to this interactive process as reflecting human-machine communication privacy management (HMCPM). Studying how users interact with social media algorithms and what affordances signal to the users that the machine is responsive to their feedback is especially helpful to see the interactive,

two-way privacy management process between humans and machines (Bucher & Helmond, 2018; Lutz, 2023; Ronzhyn et al., 2023).

Communication privacy management (CPM) theory allows a robust framework for how individuals enact strategies to control private information about themselves and what they do when their privacy expectations with machines have been violated (Petronio, 2002, 2013). In human-to-human interactions, individuals who experience a privacy violation with another person can go back to that person, sense-make about the privacy violation, and discuss privacy rules that will enable an adequate (re)balance of access to and protection of their private information going forward (Steuber & McLaren, 2015). However, exploring the human-machine context allows consideration of how users try to interface with a social media algorithm to tell it what private information is okay to know or make predictions about them (Eslami et al., 2016). Such a focus is necessary to elucidate how people respond to privacy breakdowns with machine agents. Filtering algorithms leave users in the dark when trying to understand what is stored, how it is acted on and shared, and ways to exert privacy control beyond adjusting privacy settings or completely disengaging from use.

HMC primarily focuses on meaning created between people and machines, in which machines are observed as both interlocutors with others and mediums through which communication can occur (i.e., communication with and through machines; Etzrodt et al., 2024; Guzman, 2018; Richards et al., 2022). Numerous theories from various disciplines have been used to explore how meaning is created and studied between humans and machines (Richards et al., 2022; Spence, 2019). This current study seeks to map the meaning created between the user and algorithm concerning experiences where the algorithm seems to know more than it should according to CPM's central principle of boundary turbulence and recalibration. Focusing on an HMC perspective in adapting CPM helps go beyond existing privacy research by studying the meaning created in navigating the simultaneous need for openness and maintaining control over private information. Specifically, we follow the recommendations by Petronio (2002), who states that sometimes the best way to learn about privacy management practices is to look at breakdowns. As such, we asked users to describe a time when a filtering algorithm violated their privacy expectations (privacy turbulence from CPM theory) and how they attempted to regain effective privacy management control once again (privacy recalibration strategy use). CPM theory provides a practical, theoretical process describing how individuals manage their private information that can be more fully applied to user behaviors in this context (Petronio, 2013).

Communication Privacy Management and Social Media Algorithms

One benefit of using CPM theory in this context is that it is a systems-based framework about how people manage their private information with others through articulating and utilizing privacy rules to effectively control private information (i.e., information that makes an individual feel vulnerable about the possibility of it being shared with others; Petronio, 2002). The theoretical principles of privacy ownership, privacy control, and privacy turbulence enable people to balance the simultaneous desire to be open with others and adequately protect access to their private information (Child et al., 2012; Petronio,

2013; Petronio & Child, 2020). This boundary regulation process allows for an enhanced definition of privacy that integrates human behavior in the human-algorithm context.

CPM theory notes that individuals feel they should be able to own and control private information about themselves (Durham, 2008; Frampton & Child, 2013; Petronio & Child, 2020). Nuances exist to the ownership of private information in the context of its management with social media algorithms. Specifically, as we live in an increasingly algorithmically connected world, trace data is used to predict who we are as people (Segijn et al., 2024; Segijn et al., 2025; Segijn & Van Ooijen, 2020; Strycharz et al., 2024). Because of the use of this trace data, social media users do not often think about the micro-bits of data that can feed over into use by a social media algorithm. When users do not authorize the collection of trace data to make individualized predictions, they may come to perceive a social media algorithm as having gained unauthorized access to their private information that now resides in a collective privacy boundary with the algorithm (Durham, 2008; Frampton & Child, 2013; Petronio & Child, 2020).

Once private information resides in a collective boundary, it is controlled by stipulating sharing, access, and protection rules with authorized co-owners, especially with the information residing within the collective privacy boundary perceived as more private than public (Kennedy-Lightsey et al., 2012). In the context of social media algorithms, when unauthorized access is perceived to have occurred, joint management of private information is more complex precisely because the original owner does not know how it moved into the collective privacy boundary, which can help prevent further breakdowns from occurring (Afifi, 2003; Petronio, 2013).

As social media algorithms are well integrated into daily life for users, it is important to examine how users perceive aspects of their private lives showing up in the algorithm's recommendations, leading to different breakdowns. Specifically, algorithms can take the most seemingly unobtrusive details about the user from a variety of avenues (e.g., the user directly, their location information, purchase history with other offline companies; Knijnenburg et al., 2022) and make intrusive predictions about the user to provide content and ads that lead users to feel uncomfortable, if not vulnerable to the algorithm (De Keyzer et al., 2022; Ruckenstein & Granroth, 2020; Tucker, 2014). This current research sheds light on the growing tension between users' expectations of privacy management and invasive social media algorithm practices. Identifying a typology of algorithmic privacy breakdowns can inform future research on the HMCPM process and how algorithms may be modified to allow users the control they desire over their private information—something necessary to prevent privacy breakdowns from occurring in the future. Hence, we ask:

> **RQ$_1$**: What are the types of breakdowns that users experience with social media algorithms?

When boundary turbulence occurs, CPM theory and research illustrate that engaging in repair practices by integrating new information about privacy expectations and what led someone to mark an instance as a privacy management breakdown can help in adjusting privacy management choices in ways that prevent future occurrences from happening (Petronio, 2002). For example, in relationships, one recalibration strategy post-violation

can be to cut off the violator from knowing any private information in the future (Steuber & McLaren, 2015). However, people engage in recalibration not only in personal relationships but also in various tech contexts.

Prior social media research suggests that one way users manage a lack of control of their private information is to proactively revisit content shared through social media and make deletions to content in order to prevent the further sharing of undesired information posted and to maintain adequate online disclosure and privacy management practices (Child et al., 2011). Recalibration strategies in an algorithmic context may include telling the algorithm to hide content and never show that kind of material again, changing privacy settings, or simply discontinuing the use of a social media algorithm for a short time or indefinitely (Aguirre et al., 2015; Tucker, 2014). Looking at other tech contexts, Zimmer and colleagues (2020) found that participants modify the amount of personal fitness information available for co-ownership following a triggering event, increasing their privacy management concerns. Holvoet and colleagues' (2022) research suggests that participants may limit future information disclosure or refuse to accept a privacy policy as a coping response to commercial data collection and sharing practices. Finally, users may also attempt to recalibrate their privacy by searching for random things to throw the algorithm off when its predictions get too close.

However, all of these strategies support that there is utility in learning from the breakdowns and recalibration attempts of others (DeGroot & Vik, 2017; Petronio, 2013) because when people experience a privacy breakdown, they feel embarrassed, suffer consequences at work, feel exploited by organizations, or experience unpleasant friction in their relationships (Hargittai & Marwick, 2016). Given that algorithms represent a unique kind of co-owner of private information, this second research question explores how original owners try to adjust and adapt to the perceived privacy violation in research question two:

> **RQ$_2$**: How do users of social media algorithms attempt to recalibrate privacy rules when privacy breakdowns with an algorithm occur?

Method

Participants

Following IRB approval (Kent State University IRB# 879), U.S. residents ($N = 636$) 18 years or older who reported using Facebook, TikTok, or Instagram regularly were recruited using Prolific's issue-specific sampling criterion. Participants invited to participate reported to Prolific having used all or any social media platforms: Facebook, TikTok, or Instagram. Participants were compensated a minimum of $3.00 each for the study. The sample was mostly male identifying ($n = 322$, 50.62%; 1 not reported), with ages ranging from 18 to 80 years old ($M = 36.90$; $SD = 13.28$). Regarding race, a majority of participants were White ($n = 372$, ≈ 58.49%), followed by Black ($n = 93$, ≈ 14.62%), mixed ($n = 66$, ≈ 10.38%), Asian ($n = 62$, ≈ 9.75%), and other ($n = 40$, ≈ 6.29%), with three participants (≈.47%) not providing this information to Prolific.

Procedures

Participants completed a Qualtrics survey where they responded to open-ended questions about their experiences of privacy breakdowns and the use of repair strategies with the social media algorithm. All questions were worded concordantly to focus on one of the platforms (Facebook, $n = 213$, $\approx 33.49\%$; TikTok, $n = 212$, $\approx 33.33\%$; Instagram, $n = 211$, $\approx 33.17\%$) that participants indicated they used regularly. This wording was consistent throughout each participant's survey.

Participants were asked open-ended questions corresponding to this current study's research questions. Specifically, participants were asked, "In your use of [platform], tell us about a time when a target ad or content you were recommended by the algorithm felt too personal/intimate/knows too much information," and "What about the ad or content recommended by [platform]'s algorithm made you feel it was too personal/intimate or knowing too much information?" The first question helps identify users' experiences of privacy breakdowns; however, the inclusion of the second question enhances our understanding of what specifically about the breakdown experience gave way to the user feeling the algorithm was too personal, intimate, or knew too much information about them. This information helped contextualize the kinds of breakdown experiences social media users encounter when interfacing with algorithms. To explore possible recalibration strategies employed by social media users, participants were asked, "What did you do (if anything) in response to seeing such an ad or content recommended by [platforms]'s algorithm?" Together, these open-ended questions capture, from the user perspective, the contributing factors in the algorithm's behavior that led to perceiving something as a privacy breakdown, why it violated their expectations, and what attempts or strategies users employed to overcome algorithmic privacy breakdowns.

Data Analysis

Using a derived etic content analysis approach to coding corresponding to our research questions (Neuendorf, 2002), the analysis focused on "what units make sense within the world of messages" (Neuendorf, 2002, p. 72). Participant responses were reviewed openly, and ideas and concepts corresponding to possible breakdown and recalibration types were refined through consultation with a CPM expert as a type of content validity check. The resulting ideas and concepts were further refined into a preliminary typology of privacy breakdowns and recalibration strategies. Participants articulated five types of privacy breakdowns, and six different strategies reflect participants' attempts as privacy recalibration strategies.

Each category for analysis was defined and operationalized in a codebook used to train two independent coders who read through and coded participant responses related to both research questions (Neuendorf, 2002). A participant's entire response to the breakdown and, subsequently, the recalibration question was the unit of analysis for each research question. Before independently coding 10% of the open-ended data, coders were trained and practiced coding sample open-ended responses into the coding scheme. Intercoder reliability was not reached for all categories in the first round. As such, coders were retrained by looking at disagreements, adjusting the codebook based upon the coding

from the first round, and then the coders each coded 10% of the data a second time into the coding schema. After this second round, one category required further retraining. On the third time, this final category also reached an acceptable level of intercoder reliability (Krippendorff's $\alpha \geq .70$). After intercoder reliability training and testing occurred, the two coders divided the remaining data and coded the data with the revised codebook. Intercoder reliability checks occurred between the two coders at the end of all of the coding by testing intercoder reliability estimates for 20% of the data at the end of the coding. The coders had an acceptable level of intercoder reliability at the end as well ($\alpha \geq .70$).

Results

Privacy Breakdowns With Social Media Algorithms (RQ_1)

The first research question (RQ_1) asked what types of breakdowns users experience with social media algorithms. The first code, *predictive targeting of personal searches*, was defined as users' experiences of getting content and/or ads that correspond to their previous searches (n = 195, 31%). For example, one participant remarked, "I was searching for some outdoor activities for my kids on Google, and when I opened my [platform], I got several ads for activity ideas for kids and also some places to go for recreations [sic] with kids." The range of private information predicted by participants' online searches spans from the mundane to sometimes deeply personal and even assumed explicitly private. Regarding a profoundly personal matter, one participant wrote, "I had recently been browsing for some workout and weight loss tips when I started receiving ads for diets, gym memberships, and self-proclaimed personal trainers who knew one simple trick to help lose weight and get shredded fast. It felt pretty invasive and only served to hurt my self-esteem even more."

The second code, *environmental listening/surveillance/interference*, was used to capture instances in which participants recalled getting content or ads related to previous conversations with other people that did not occur over a medium as if they were being surveilled (e.g., face-to-face conversations; n = 176, 28%). For example, one participant shared their experience of getting recommended ads or content related to their sexual health that they had talked about in the bedroom with their sexual partner, "I recently had trouble getting 'it up' during a hookup. My phone was beside the bed. The next day I started getting ads for Viagra, which appalled me." When asked what about the ad or content made them feel it was too personal/intimate or knowing too much information, that same participant remarked, "First, that it was listening to what I was saying, not just picking up things that I had searched. Second, that it was an intimate topic."

Within this type of breakdown, participants would share that they would have sexual health and general health conversations with other people, including a medical provider, only to then immediately receive ads related to the medical conversation. For example, one participant recalled, "I once described to my therapist about how I would daydream a lot in school to distract myself from my anxiety. Within the next few days, I got [content on platform feed] about maladaptive daydreaming even though I had never looked up anything related to it on my phone." When asked why they felt the algorithm knew too much information, the participant explained, "since it was something related to my mental health I felt as though a boundary was overstepped. I don't want [platform] to be

able to know what mental health issues may apply to me. If an app can pick up that information and I don't know what the app does with the information—I am not comfortable with it." As another example, one participant about a topic related to conceiving children explained, "I was discussing ovulation sticks with my partner and afterwards I got a few targeted ads from scrolling on my feed on Clearblue digital ovulation sticks . . . It was just too specific in a personal conversation and I had not searched for any information regarding it." These above examples highlight the perception of a privacy breakdown related to non-mediated communication with other people.

Several participants recalled receiving recommended ads or content from their social media algorithm, primarily relevant to health-related private aspects of their lives. This was best captured with the third code, *exploitation of health and emotionally vulnerable health-related private information*, which included instances of personalized ads or content that seem to exploit user health data or things about their overall health that left them feeling emotionally vulnerable to seeing it encapsulated in an advertisement (n = 150, 24%). For example, a participant referencing their health condition remarked, "I have a sensitive health condition and after using a telehealth service that treats this specific condition, [platform] started showing me ads for a supplement company that claims to treat it." Responding to the probing question to capture *why* such an ad or content felt like the algorithm knew too much information, the participant explained, "I don't like that a social media company could have a lot of my health data. My health is personal and something that I feel should be between me and my doctor and maybe my family and friends if I choose to share." In another example, one participant claimed, "I see vibrator ads which I feel is inappropriate. They pop up daily. I don't know how to get rid of them and how they found a way on my feed." However, one of the most provocative comments in this category concerned a participant in their experience on social media following a very recent miscarriage, "I just had a miscarriage and I saw on my [feed] a jewelry store that made miscarriage memorial necklaces." The intimate nature of these health-related recommended ads or content highlights the complexity of the unique boundaries participants desire, depending on the context of the predicted information.

The fourth code *cross-platform privacy breaches* captured instances in which users reported receiving recommended ads and/or content related to previous conversations with other people via mediated channels (e.g., phone, text messages, email, instant messenger; n = 22, 3%). For example, participants would recall having conversations about family health issues on the platform's personal messages feature and then getting advertised and recommended content related to a disease that was discussed, "I was asking my brother on [platform] messenger about a family concern and disease. Later on, I was getting ads for that very subject, so I know I was being watched even with messages that should be private." Another participant remarked, "I was getting ads related to mental health services. It felt very invasive since I was just having a private texting conversation with a friend about that topic."

When referring to the breakdown, participants would share their confusion about how their conversation on a completely different platform could lead to targeted ads on another. One participant's comment best encapsulates this finding, "I was talking to a friend on the instant messaging application called Discord about haircare. A day later, I started getting haircare advertisements on Instagram, when these two services should be

entirely separate," and when asked what about this led them to feel the algorithm knew too much, they remarked, " . . . it made me feel like my privacy was being violated."

During the preliminary review of the data, there were several instances in which participants talked about experiencing a breakdown even though they were cautious about avoiding it in the first place. This was best captured with the fifth breakdown code, *perceived breach despite precautions*, representing instances in which participants had a breakdown in privacy management, which occurred even though the participant felt confident they took steps or were careful about allowing information to be shared with the platform. However, when coding for this in the dataset, specifically regarding the open-ended questions, occurrences were seldom or non-existent (n = 10, 2%). Because of the exploratory nature of the data collection and to allow for further analysis, coders were instructed to use a specific category for when the participant's response to the breakdown questions does not fit with the pre-defined codes (n = 83; 13%). Table 1 in the supplementary materials provides a synopsis overview of the breakdown codes (https://osf.io/b2vsy/?view_only=2cded04eaa3f4eb3ad71604a478f5a2e).

Privacy Recalibration Strategies With Social Media Algorithms (RQ_2)

Research question two (RQ_2) asked how users recalibrate to effective privacy management following a privacy breakdown with their social media algorithm. Specifically, RQ_2 asked how do users of social media algorithms attempt to recalibrate privacy rules when privacy breakdowns with algorithms occur? Content analysis was used to examine RQ_2 through coding procedures to help illuminate how users seek to repair the collective boundary with their social media algorithms following a privacy breakdown.

Regarding recalibration strategies and/or practices, six categories were thought to best capture participants' responses to experiencing privacy breakdowns with their social media algorithms. The first category, *passive coping,* best represented instances in which participants would try to ignore the breakdown, scroll past it, and even express emotional responsiveness, like feeling defeated (n = 317, 50%). For example, participants would acknowledge the targeted ads or content but then move on with their scrolling behavior, saying, "I'm normally like here we go again. I [watch the video] then skip." This was present in other responses from participants. For instance, one participant wrote, "Nothing, I just scrolled past it and rolled my eyes," and another responded, "I felt conflicted because I appreciated the advice given but I felt also like targeted so I just kept going."

In the second category, *active boundary management* (n = 142, 22%) reflects instances where participants tried to adjust the boundary by directly interfacing with the algorithm. They would avoid liking certain content that would signal private information to the algorithm, report ads or content as irrelevant, or change their settings on the platform account or device. For example, talking about avoiding signaling to the platform that its prediction about them was accurate, one participant explained, "I made sure not to like it or interact with it so that [platform] wouldn't think it was on to something." In another example, one participant shares their effort in re-orienting the algorithm by avoiding explicit content related to their sexuality, "I usually get news feeds. I'm gay. I liked to watch gay men dancing to choreographed routines. Eventually, I started getting highly suggestive feeds . . . almost gay porn. I did not stay on any of these sites. Slowly, my feeds returned to

the content that I like." Participants also shared that after experiencing a breakdown with their social media algorithm, they would take action by being careful about their interactions around their devices and altering their privacy settings on the platform. For instance, "[I]n response to the targeted ad, I became more cautious about discussing certain topics around my phone. I also reviewed and adjusted my privacy settings on [platform] to limit data sharing and personalized ad targeting."

Several participants would talk about adjusting their settings to avoid inadvertently sharing their private information, such as closing or deleting their search history, cookies, clearing their cache on their web browser, and even verifying that their microphone and other physical features of their phones that could have captured their private information were not active. This is best encapsulated by this participant's response to the question about what they did in response to the breakdown, "I closed all of my search history related to what I was looking for. I updated my settings on [platform] to take off my microphone, and I deleted the cookies on my phone to make sure that there was nothing being stored or tracked through my phone."

Discussions with friends and family were one strategy individuals used to try to recalibrate their privacy boundaries with their social media algorithm, which was observed as *social validation and knowledge seeking* (n = 45, 7%). For instance, one participant remarked, "we talked about how weird it was and kept showing each other the videos the other had just watched pop up on our [feed]," while another stated, "I was shocked and a bit freaked out so I told my mom about it and she was a bit freaked out too."

Contrary to passive coping, *boundary resets*, account for occurrences when participants deleted the platform app, stopped using the platform, or took some form of action that severed the privacy boundary (n = 26, 4%). Most often, for participants, this meant stepping away from the platform and eventually walking back toward the platform—however, with hesitation or more care about the information allowed to be shared with the algorithm. For instance, one participant explained, "I deleted the app for a while. It felt really personal and creepy to be honest. I deleted it for a couple weeks. I am back on it now. But with lots of reserve [sic] about it." This type of response is reflected in the experiences of other participants as well, for example, one participant remarked, "I deleted that app and eventually redownloaded it and it scares me to this day," and another explained, "I was a little creeped out; I didn't use it for a couple of days after that, and I even removed it from my phone."

Identified as *tradeoff acceptance/resignation*, participants would remark that they felt taking action was pointless or were unsure what to do at this point. This code had a high percentage of agreement among coders (intercoder agreement = 97.76%). However, this code was found to have low intercoder reliability from the content analysis. To highlight participant quotes that encapsulate this code, one participant wrote, "There were a couple of ads, I can't remember what they were, but they kept rotating around and around and around and wouldn't go away on [platform] so there is an area that you click on to block these and you won't see those ads anymore, however, more ads just kept showing up so it's sort of pointless." Or put another way, one participant remarked, "I don't believe I could control it once it is in [platform]'s database regardless of what they may say publicly." Some participants would also recall the tradeoff for using the platform in exchange for private information (e.g., tradeoff fallacy), for instance, as put by one participant, "I try to ignore it

and just assume thats [sic] its part of life If I want to use the internet and social media [sic]. It's the price we all pay for technology." This category best reflects the conscious toleration of surveillance capitalism.

Finally, while it was thought that similar to Metzger (2007), we would find instances in which users might try to trick their social media algorithm as a response to experiencing a privacy breakdown, such as *creative resistance/subversion*, this was a seldom occurrence (n = 1; < 1%). Similarly to the breakdown codes, independent coders were instructed to use a special code to indicate when a participant's response did not match the existing pre-defined codes (n = 82; 13%). Table 2 in the supplementary materials contains an overview synopsis of the recalibration codes (https://osf.io/b2vsy/?view_only=2cded04eaa3f4eb3ad71604a478f5a2e).

Discussion

This study focused on privacy breakdowns and recalibration strategies with social media algorithms. According to CPM theory, privacy breakdowns and recalibration strategies are some of the most informative parts of the privacy management process (Petronio, 2013; Steuber & McLaren, 2015). This comes from the fact that some individuals do not fully grasp their norms for privacy management until they experience a privacy breakdown where their expectations have not been met. This current work is foundational for understanding privacy management in human-machine communication (or HMCPM), has important implications for future research, and corresponds to existing literature surrounding privacy, advertising, and social media algorithms.

First, participants' recalibration practices broadly showcase users' adaptive responses to privacy turbulence. For instance, in response to algorithmic privacy breakdown experiences, participants would engage in boundary resets and active boundary management. Users in this study who engage in boundary resets, or a more extreme form of ceasing co-ownership with the algorithm, likely do so out of a lack of straightforward tools provided by social media companies to allow individuals to engage in more data co-ownership with an algorithm. If such tools existed, individual users could more actively manage the kind of private information an algorithm can and should act on and what micro-bits of information should be forgotten and not acted upon. Given the lack of features and tools for data co-ownership, the costs for these users associated with algorithmic co-ownership of unauthorized private information outweigh any benefits that may occur from personalized advertising and allowing the algorithm to co-own any of their private information going forward. This cost-benefit analysis from CPM theory (Petronio & Child, 2020) is similar to the privacy calculus model, where people actively consider the pros and cons of allowing greater access to their information. People may also engage in boundary resets by deleting and then sometimes re-downloading a social media app because they perceive that the algorithm has been cleared with the redownload, essentially providing them another opportunity to curate their feed as desired and have their private information managed according to their desires. Again, other research frameworks, like folk theories, may be instrumental in expanding users' interpretation of why they perceived that a boundary reset and redownload may work in terms of engagement with social media algorithmic systems.

In contrast to those who cease co-ownership with the algorithm (through persisting with rigid boundary resets), many users engaged in other types of boundary coordination attempts following a privacy breakdown experience. Specifically, participants in our study adjusted and fine-tuned their privacy settings on the platform and deleted some of the private information an algorithm stored about them (i.e., clearing ad categories). CPM theory suggests that individuals seek to repair the privacy boundary following a breakdown to arrive at different privacy management practices in the future than what led to the privacy breakdown. As such, we learn a lot about people's privacy management expectations by examining when a privacy regulation system with an algorithm is out of alignment (Petronio, 2002, 2013; Steuber & McLaren, 2015). Because of this, we see in our data the interactive nature between human and machine agents to try to arrive at CPM's self-regulating principle (DeVito et al., 2018; Eslami et al., 2016; Holvoet et al., 2022; Taylor & Choi, 2024).

Prior work concerning algorithmic literacy would conceptualize users' understanding and ability to use algorithms comprising affective, cognitive, and behavioral dimensions (Oeldorf-Hirsch & Neubaum, 2023). In the context of our study, it is likely that breakdown experiences not only inform recalibration strategies but also impact the users' attitudes toward social media algorithms (affective) and their awareness of algorithmic functioning (cognitive) that plays a role in how they regulate the privacy with an algorithm. The results of the current study offer theoretical insights into privacy management practices in the human-machine context or human-machine communication privacy management practices (HMCPM). As seen in other CPM-based research, individual privacy management with social media algorithms begins with the individual and what information they are comfortable with others knowing in collectively owned and managed privacy boundaries. This dynamic is more complicated when moving private information from human-to-machine versus human-to-human communication.

Second, passive coping strategies for privacy management highlight the increased tension between user agency and algorithmic constraints. Recalibration with social media algorithms is complicated as they are not only subject to change, but social media platforms are not fully transparent about why the user was provided a specific recommended content or advertisement (e.g., only telling the user vague demographic targets) or how that information that is now co-owned by the algorithm is being acted upon. Algorithmic opacity (i.e., the algorithmic decision-making process is not transparent to the user) can be frustrating and lead to increased fatigue and even resignation of privacy management (Hargittai & Marwick, 2016; Turow et al., 2015).

Resignation in this context stems from the feeling that privacy violations are unavoidable when interacting with an algorithm because it uses predictive associations based on data not transparently shared with individual users. When a system like an algorithm is semi-closed, managing private information with an algorithm can feel pointless (Hargittai & Marwick, 2016; Turow et al., 2015; van der Schyff et al., 2023). That is because they cannot tell an algorithm about how they want it to store, track, and ignore content about them in desired ways or even know the algorithm's decision-making process; the end user feels that engaging in correcting their privacy boundary is futile. Future research is needed regarding the impact of repeated experiences of privacy breakdowns on social media and psychological variables (e.g., loneliness, privacy fatigue; Taylor & Choi, 2024; Yang et al., 2024).

Participants frequently mentioned receiving targeted advertisements and recommended content relevant to their online activity outside the platform (e.g., private browsing history). It is possible that users still do not come to expect these types of breakdowns. This lack of expectations about the algorithm may stem from users being engaged in a *fuzzy privacy boundary* (Child & Starcher, 2016), in which the audience comprised of known and unknown individuals is collapsed contextually to represent one general audience who may have access to user data (Child & Westermann, 2013; Miller et al., 2016). People do not expect known or unknown third parties to listen in on their conversations and take advantage of a fuzzy privacy boundary to disclose that private information elsewhere in an unauthorized fashion (Petronio, 2002, 2013). Future work may consider how users view the co-ownership of private information with social media algorithms and to what extent privacy breakdowns predict co-ownership in this context.

Third, our findings have broader implications for algorithm design, including user-driven transparency features and tools for boundary coordination. Greater transparency in algorithmic design holds significant potential for mitigating the adverse effects found in our analysis. If users were more clearly informed about how specific recommendations are made—such as clearly communicated explanations about what user behaviors triggered particular ads or suggested content—then uncertainty, confusion, and misattribution could substantially decrease. This way, algorithmic transparency could help users develop more accurate and informed understandings of their online privacy boundaries. Consequently, recalibration strategies could evolve from predominantly passive coping responses toward more active, empowered privacy management behaviors.

The issue of algorithmic opacity among many of our participant breakdown experiences speaks to existing calls for increased transparency in algorithms (Diakopoulos, 2014). Social media users are getting personalized advertising related to their private information. CPM theory notes that in the context of privacy management, users expect to be able to own and control any private information about themselves (Petronio, 2002). Not knowing what an algorithm has stored, how accurate those micro-bits of data are to the individual, and how that information gets managed by an algorithm complicates the interactive privacy management process, leaving individuals few options for coordinating their private information. While this current study did not evaluate the extent to which certain breakdowns corresponded with particular recalibration strategies, it would be important for future work to consider measuring both and determining how people gravitate to specific recalibration strategies over others and what are the conditions necessary for breakdowns in this context to happen in the first place. For example, an individual's folk theories may be inaccurate, leading to perceptions of breakdowns. Because recalibration strategies respond to a particular breakdown, the users' interpretation of the system may influence their enhanced understanding of regaining control over their private information.

In practice, this means that an algorithm may make an educated guess about someone's identity based on geolocation data or other micro-bits of data that could be inaccurate and introduce bias into advertisement practices and information provided to the user. On the other hand, the algorithmic predictions may be accurate and preempt any disclosure practices by the individual, which does not allow them to control and manage information about themselves, which is a fundamental assumption for how people feel about the management of their private information as a primary owner (Petronio, 2002, 2013; Petronio &

Child, 2020). As such, greater algorithmic transparency can limit bias and provide users a more equitable and fair opportunity to be a more active owner of their private information and predictions about them from micro-bits of data stored by algorithmic systems.

Should platforms fail to implement meaningful transparency enhancements, it is also possible that users will rely heavily on folk theories that are shaped by incomplete or inaccurate assumptions about algorithms. This reliance may perpetuate feelings of resignation and fatigue, weakening their perceived control and diminishing their agency in privacy management contexts. Users might increasingly view recalibration efforts as futile, exacerbating privacy fatigue and dissatisfaction with algorithmic co-ownership of their data. Moreover, future research should seek to understand some of the core and catalyst influences on individuals' willingness to co-own private information with social media algorithms. This current analysis of participant experiences illustrates that becoming aware of unauthorized access to private information may contribute to whether users desire co-ownership with their social media algorithm. However, what remains to be tested is a comprehensive evaluation of privacy management in the social media algorithm context that determines under what conditions being aware of algorithms informs rules regulating co-ownership. Our analysis would suggest that privacy fatigue may play a role in individuals' willingness to promote co-ownership. Specifically, those who are highly aware of algorithms from their breakdown experiences may not be as willing to allow co-ownership; however, privacy fatigue may hinder the motivation (e.g., van der Schyff et al., 2023).

Research suggests that algorithm transparency may not have as strong of an intervening role in how users manage private information with an algorithm. However, it can help them feel more in control of their private information. For instance, Segijn and colleagues' (2021) review of personalized transparency and control in online privacy management research suggests that greater transparency on the part of the algorithm and platform does not necessarily lead to users being able to control their private information effectively. Our findings correspond to the need for additional research concerning the relationship between breakdowns and recalibration practices depending on different variations of algorithmic transparency. The challenge for social media designers and policymakers lies in prioritizing transparent human-machine communication strategies. Such transparency could potentially restore user confidence, enhance effective privacy management in this context, and fundamentally reshape user-algorithm interactions toward healthier and more equitable engagements.

Limitations of the Study

There is obviously more analysis to do regarding the open-ended responses in this study. As a limitation of this study's findings, coders could indicate if an open-ended response did not match any predefined codes listed in the codebook. The codes presented to them were neither fully exhaustive nor exclusive (Neuendorf, 2002). Because of this, coders indicated a low number of cases (≈13% for breakdowns and ≈13% for recalibration practices) as not applicable to any of the codes. However, responses that did not apply to the other codes better reflected participants indicating they did not have such an experience (e.g., breakdown in privacy management) or the response was unrelated to the question being asked. The intercoder reliabilities for the N/A breakdown and N/A recalibration

codes were .69 and .77, respectively. While an alpha of .69 is not above or equal to .70, it is cited as acceptable for tentative conclusions (Krippendorff, 2004a, 2004b). Within those responses marked "response not applicable," follow-up analysis may be needed to work toward illustrating additional codes present in these data that reflect experiences of privacy breakdowns and recalibration practices used in response to breakdowns. Some codes may coexist with other codes (e.g., exploitation of health and emotionally vulnerable health-related private information can also be related to cross-platform privacy breaches). Future research may seek to explore the co-occurrence of our identified breakdown and recalibration typologies (e.g., Geisler, 2018) and how experiences of one or several kinds of breakdowns relate to a user's overall level of privacy management (Petronio & Child, 2020).

Conclusion

Users' experiences of privacy breakdowns with social media algorithms often reflect receiving targeted ads and recommended content that eerily relate to previous private conversations with other people and other online behavior. In response to these breakdowns, users seek to sever the collective boundary (disallow further co-ownership), liking other content, or avoid engaging with or spending too much time on the recommended ad or content, or lean in to adjust their collective boundary through the use of settings. These findings provide insight into users' issues managing private information with the algorithm and how these different privacy breakdowns lead to certain recalibration practices. These results inspire future work investigating human-machine communication privacy management (HMCPM).

Author Biographies

Matthew J. A. Craig (PhD, Kent State University) is an Assistant Professor in the School of Communication, Journalism, and Media at Central Michigan University. His research interests include human-machine communication and computer-mediated communication. Recent publications of Craig's include articles in *Telematics and Informatics*, *Computers in Human Behavior: Artificial Humans*, *Human-Machine Communication*, *Communication Quarterly*, and *Communication Studies*. Craig is also a lab faculty member of the Communication and Social Robotics Labs (www.combotlabs.org) and leads the COMBOTLABS-CMU in the School of Communication, Journalism, and Media at Central Michigan University.

https://orcid.org/0000-0002-4824-566X

Jeffrey T. Child (PhD, North Dakota State University) is a Professor and Chair of the Department of Communication Studies at the University of Nevada, Las Vegas. He is a former editor of the *Journal of Family Communication* and current President of the Central States Communication Association. His research explores privacy regulation and disclosure practices in personal and mediated spaces, and how people respond to privacy breakdowns and engage in privacy recalibration practices. His research has been published in a range of journals.

Author Note

Research reported in this publication was supported by Kent State University's College of Communication & Information Research and Creative Activity Grant and Kent State University's Graduate Student Senate Research Grant. Data used in this manuscript were part of the first author's dissertation work.

Acknowledgments

This work was heavily inspired by Dr. Sandra Petronio's work in theorizing Communication Privacy Management theory (Petronio, 2002, 2013). While completing this research, which is one part of several studies and analyses, Sandra unfortunately passed away on April 20, 2024. Without her pivotal original work, this research would not have been possible. Sandra was a phenomenal systems thinker, and we are honored to continue advancing her work.

References

Afifi, T. D. (2003). 'Feeling caught' in stepfamilies: Managing boundary turbulence through appropriate communication privacy rules. *Journal of Social and Personal Relationships*, *20*(6), 729–755. https://doi.org/10.1177/0265407503206002

Aguirre, E., Mahr, D., Grewal, D., De Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, *91*(1), 34–49. https://doi.org/10.1016/j.jretai.2014.09.005

Auxier, B., & Anderson, M. (2021). Social media use in 2021. *Pew Research Center*. https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/

Bucher, T., & Helmond, A. (2018). The affordances of social media platforms. In J. Burgess, A. Marwick, & T. Poell (Eds.), *The SAGE Handbook of Social Media* (pp. 233–254). SAGE.

Child, J. T., Haridakis, P. M., & Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior*, *28*(5), 1859–1872. https://doi.org/10.1016/j.chb.2012.05.004

Child, J. T., Petronio, S., Agyeman-Budu, E. A., & Westermann, D. A. (2011). Blog scrubbing: Exploring triggers that change privacy rules. *Computers in Human Behavior*, *27*(5), 2017–2027. https://doi.org/10.1016/j.chb.2011.05.009

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. https://doi.org/10.1016/j.chb.2015.08.035

Child, J. T., & Westermann, D. A. (2013). Let's be Facebook friends: Exploring parental Facebook friend requests from a communication privacy management (CPM) perspective. *Journal of Family Communication*, *13*(1), 46–59. https://doi.org/10.1080/15267431.2012.742089

DeGroot, J. M., & Vik, T. A. (2017). "We were not prepared to tell people yet": Confidentiality breaches and boundary turbulence on Facebook. *Computers in Human Behavior*, *70*, 351–359. https://doi.org/10.1016/j.chb.2017.01.016

De Keyzer, F., van Noort, G., & Kruikemeier, S. (2022). Going too far? How consumers respond to personalized advertising from different sources. *Journal of Electronic Commerce Research*, *23*(3), 138–159. http://www.jecr.org/sites/default/files/2022vol23no3_Paper1.pdf

DeVito, M. A., Birnholtz, J., Hancock, J. T., French, M., & Liu, S. (2018). How people form folk theories of social media feeds and what it means for how we study self-presentation. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1–12). https://doi.org/10.1145/3173574.3173694

Diakopoulos, N. (2014). *Algorithmic accountability reporting: On the investigation of black boxes*. Tow Center for Digital Journalism. https://www.cjr.org/tow_center_reports/algorithmic_accountability_on_the_investigation_of_black_boxes.php

Diakopoulos, N. (2019). *Automating the news: How algorithms are rewriting the media*. Harvard University Press.

Dolin, C., Weinshel, B., Shan, S., Hahn, C. M., Choi, E., Mazurek, M. L., & Ur, B. (2018). Unpacking perceptions of data-driven inferences underlying online targeting and personalization. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1–12). ACM. https://doi.org/10.1145/3173574.3174067

Drüeke, R., & Peil, C. (2024). Autonomy and agency in farming: Exploring human, machine, and animal dynamics. *Human-Machine Communication*, *9*(1), 101–124. https://doi.org/10.30658/hmc.9.7

Durham, W. T. (2008). The rules-based process of revealing/concealing the family planning decisions of voluntarily child-free couples: A communication privacy management perspective. *Communication Studies*, *59*(2), 132–147. https://doi.org/10.1080/10510970802062451

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 19–32). Springer.

Eslami, M., Karahalios, K., Sandvig, C., Vaccaro, K., Rickman, A., Hamilton, K., & Kirlik, A. (2016). First I "like" it, then I hide it: Folk theories of social feeds. In *Proceedings of the 2016 CHI conference on human factors in computing systems* (pp. 2371–2382). http://dx.doi.org/10.1145/2858036.2858494

Eslami, M., Rickman, A., Vaccaro, K., Aleyasen, A., Vuong, A., Karahalios, K., Hamilton, K., & Sandvig, C. (2015). "I always assumed that I wasn't really that close to [her]" reasoning about invisible algorithms in news feeds. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems* (pp. 153–162). http://dx.doi.org/10.1145/2702123.2702556

Etzrodt, K., Kim, J., van der Goot, M. J., Prahl, A., Choi, M., Craig, M. J., Dehnert, M., Engesser, S., Frehmann, K., Grande, L., Leo-Liu, J., Liu, D., Mooshammer, S., Rambukkana, N., Rogge, A., Sikström, P., Son, R., Wilkenfeld, N., Xu, K., Zhang, R., Zhu, Y., & Edwards, C. (2024). What HMC teaches us about authenticity. *Human-Machine Communication*, *8*, 227–251. https://doi.org/10.30658/hmc.8.11

Frampton, B. D., & Child, J. T. (2013). Friend or not to friend: Coworker Facebook friend requests as an application of communication privacy management theory. *Computers in Human Behavior*, *29*(6), 2257–2264. https://doi.org/10.1016/j.chb.2013.05.006

Geisler, C. (2018). Coding for language complexity: The interplay among methodological commitments, tools, and workflow in writing research. *Written Communication*, *35*(2), 215–249. https://doi.org/10.1177/0741088317748590

Gillespie, T. (2014). The relevance of algorithms. In T. Gillespie, P. J. Boczkowski, & K. A. Foot (Eds.), *Media technologies: Essays on communication, materiality, and society* (pp. 167–193). https://doi.org/10.7551/mitpress/9042.003.0013

Guzman, A. L. (2018). What is human-machine communication, anyway? *Human-machine communication: Rethinking communication, technology, and ourselves*. Peter Lang.

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 3737–3757.

Heimlich, R. (2012). Internet users don't like targeted ads. *Pew Research Center*. https://www.pewresearch.org/short-reads/2012/03/13/internet-users-dont-like-targeted-ads/

Holvoet, S., De Jans, S., De Wolf, R., Hudders, L., & Herrewijn, L. (2022). Exploring teenagers' folk theories and coping strategies regarding commercial data collection and personalized advertising. *Media and Communication*, *10*(1), 317–328. https://doi.org/10.17645/MAC.V10I1.4704

Kennedy-Lightsey, C. D., Martin, M. M., Thompson, M., Himes, K. L., & Clingerman, B. Z. (2012). Communication privacy management theory: Exploring coordination and ownership between friends. *Communication Quarterly*, *60*(5), 665–680. https://doi.org/10.1080/01463373.2012.725004

Knijnenburg, B. P., Page, X., Wisniewski, P., Lipford, H. R., Proferes, N., & Romano, J. (2022). *Modern socio-technical perspectives on privacy*. Springer Nature. https://doi.org/10.1007/978-3-030-82786-1

Krippendorff, K. (2004a). *Content analysis: An introduction to its methodology*. SAGE.

Krippendorff, K. (2004b). Reliability in content analysis: Some common misconceptions and recommendations. *Human Communication Research*, *30*(3), 411–433. https://doi.org/10.1111/j.1468-2958.2004.tb00738.x

Lee, A. Y., Mieczkowski, H., Ellison, N. B., & Hancock, J. T. (2022). The algorithmic crystal: Conceptualizing the self through algorithmic personalization on TikTok. *Proceedings of the ACM on human-computer interaction*, *6*, 1–22. https://doi.org/10.1145/3555601

Leon, P. G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., Bauer, L., Christodorescu, M., & Cranor, L. F. (2013). What matters to users? Factors that affect users' willingness to share information with online advertisers. In *Proceedings of the Ninth Symposium on usable privacy and security* (pp. 1–12). https://doi.org/10.1145/2501604.2501611

Lutz, C. (2023). Privacy and human-machine communication. In A. L. Guzman, S. Jones, & R. McEwan (Eds.), *The SAGE handbook of Human-Machine Communication* (pp. 310–317). SAGE.

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, *12*(2), 335–361. https://doi.org/10.1111/j.1083-6101.2007.00328.x

Miller, J. H., Danielson, C., Parcell, E. S., Nicolini, K., & Boucher, T. (2016). Blurred lines: Privacy management, family relationships, and Facebook. *Iowa Journal of Communication*, *48*(1), 4–22.

Neuendorf, K. A. (2002). *The content analysis guidebook*. SAGE.

Oeldorf-Hirsch, A., & Neubaum, G. (2023). What do we know about algorithmic literacy? The status quo and a research agenda for a growing field. *New Media & Society*, Article 14614448231182662. https://www.doi.org/10.1177/14614448231182662

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Suny Press.

Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication*, *13*(1), 6–14. https://doi.org/10.1080/15267431.2013.743426

Petronio, S., & Child, J. T. (2020). Conceptualization and operationalization: Utility of communication privacy management theory. *Current Opinion in Psychology*, *31*, 76–82. https://doi.org/10.1016/j.copsyc.2019.08.009

Richards, R. J., Spence, P. R., & Edwards, C. C. (2022). Human-machine communication scholarship trends: An examination of research from 2011 to 2021 in communication journals. *Human-Machine Communication*, *4*, 45–62. https://doi.org/10.30658/hmc.4.3

Ronzhyn, A., Cardenal, A. S., & Batlle Rubio, A. (2023). Defining affordances in social media research: A literature review. *New Media & Society*, *25*(11), 3165–3188. https://https://doi.org/10.1177/14614448221135187

Ruckenstein, M., & Granroth, J. (2020). Algorithms, advertising and the intimacy of surveillance. *Journal of Cultural Economy*, *13*(1), 12–24. https://doi.org/10.1080/17530350.2019.1574866

Segijn, C. M., Kim, E., & van Ooijen, I. (2024). The role of perceived surveillance and privacy cynicism in effects of multiple synced advertising exposures on brand attitude. *Journal of Current Issues & Research in Advertising*, 1–17. https://doi.org/10.1080/10641734.2024.2318711

Segijn, C. M., Strycharz, J., Riegelman, A., & Hennesy, C. (2021). A literature review of personalization transparency and control: Introducing the transparency-awareness-control framework. *Media and Communication*, *9*(4), 120–133. https://doi.org/10.17645/mac.v9i4.4054

Segijn, C. M., Strycharz, J., Turner, A., & Opree, S. J. (2025). "My phone must be listening!": Peoples' surveillance beliefs around devices "listening" to offline conversations in the US, the Netherlands, and Poland. *Big Data & Society*, *12*(2), Article 20539517251337102. https://doi.org/10.1177/20539517251337102

Segijn, C. M., & Van Ooijen, I. (2020). Perceptions of techniques used to personalize messages across media in real time. *Cyberpsychology, Behavior, and Social Networking*, *23*(5), 329–337. https://doi.org/10.1089/cyber.2019.0682

Spence, P. R. (2019). Searching for questions, original thoughts, or advancing theory: Human-machine communication. *Computers in Human Behavior*, *90*, 285–287. https://doi.org/10.1016/j.chb.2018.09.014

Springer, A., Hollis, V., & Whittaker, S. (2017). Dice in the black box: User experiences with an inscrutable algorithm. In *AAAI 2017 Spring Symposium on Designing the User Experience of Machine Learning Systems Technical Reports SS-17-04* (pp. 427–430). Association for the Advancement of Artificial Intelligence.

Steuber, K. R., & McLaren, R. M. (2015). Privacy recalibration in personal relationships: Rule usage before and after an incident of privacy turbulence. *Communication Quarterly*, *63*(3), 345–364. https://doi.org/10.1080/01463373.2015.1039717

Strycharz, J., Maslowska, E., & Kim, S. J. (2024). Computational advertising: Where are we and where are we going? Note from editors. *Journal of Current Issues & Research in Advertising*, *45*(3), 277–281. https://doi.org/10.1080/10641734.2024.2381395

Taylor, S. H., & Choi, M. (2024). Lonely algorithms: A longitudinal investigation into the bidirectional relationship between algorithm responsiveness and loneliness. *Journal of Social and Personal Relationships*, *41*(5), 1253–1278. https://doi.org/10.1177/02654075231156623

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, *51*(5), 546–562. https://doi.org/10.1509/jmr.10.0355

Turow, J., Hennessy, M., & Draper, N. (2015). *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation*. Annenberg School of Communication, University of Pennsylvania.

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy: Perceptions of online behavioral advertising. In *Proceedings of The Eighth Symposium on Usable Privacy and Security* (pp. 1–15). ACM. https://doi.org/10.1145/2335356.2335362

van der Schyff, K., Foster, G., Renaud, K., & Flowerday, S. (2023). Online privacy fatigue: A scoping review and research agenda. *Future Internet*, *15*(5), 1–31. https://doi.org/10.3390/fi15050164

Yang, H., Li, D., & Hu, P. (2024). Decoding algorithm fatigue: The role of algorithmic literacy, information cocoons, and algorithmic opacity. *Technology in Society*, *79*, Article 102749. https://doi.org/10.1016/j.techsoc.2024.102749

Zimmer, M., Kumar, P., Vitak, J., Liao, Y., & Chamberlain Kritikos, K. (2020). 'There's nothing really they can do with this information': Unpacking how users manage privacy boundaries for personal fitness information. *Information, Communication & Society*, *23*(7), 1020–1037. https://doi.org/10.1080/1369118X.2018.1543442