Int. J. Human–Computer Studies 208 (2026) 103599

Contents lists available at ScienceDirect

International Journal of Human - Computer Studies

journal homepage: www.elsevier.com/locate/ijhcs

Strategic misdirection: Attempts to protect privacy with made-up email addresses

Sharmin Ahmed [a], Emilee Rader [b], Sameer Patil [a,*]

[a] University of Utah, Salt Lake City, UT 84112, USA
[b] University of Wisconsin–Madison, Madison, WI 53706, USA

HIGHLIGHTS

- Explores how people use made-up email addresses for privacy and information overload.
- Describes interdependent privacy issues in using made-up email addresses.
- Connects email privacy practices to key privacy-related theories.
- Proposes unified client-side management for misdirected and unwanted email messages.
- Advocates input validation and double opt-in for email address collection.

ARTICLE INFO

Keywords:
Email messages
Made-up email address
Fake email address
Information overload
Unsubscribe
Interdependent privacy
Boundary management

ABSTRACT

People are often asked to provide their email addresses for identification, authentication, or communication purposes. In many such circumstances, people provide made-up email addresses instead of their own. To understand why people provide made-up email addresses, we interviewed 20 people who reported doing so. We found that the participants provided made-up email addresses to avoid information overload and protect privacy. The participants chose to provide made-up email addresses based on several factors, such as the context, personal benefits and risks, past experiences, and verification requirements. When composing made-up email addresses, the participants employed several common patterns based on their mental models of email address formats and threat models for undesirable uses of their email addresses. The participants reported using these patterns strategically to navigate the social expectations to comply with such requests and to avoid embarrassment from being perceived as deceptive. We connect our findings to email privacy more broadly through the theoretical perspectives of boundary regulation, communication privacy management, contextual integrity, social desirability, and interdependent privacy. Our insight points to design and regulatory suggestions to address the interdependent privacy issues resulting from made-up email addresses and to help users deal more effectively with email overload and email marketing.

1. Introduction

Email use is ubiquitous and essential, and for many people, mandatory. Billions across the globe rely on email (Bentley et al., 2017; Hsiao and Bentley, 2021), with an annual growth of 3 % in new email accounts (The Radicati Group, Inc., 2023). An email address, by design, allows *anyone* to send a message to that address. The open reachability helps enable communication, but also allows unwanted communication that is difficult to prevent. Providing an email address to another party can expose a person to potential privacy violations, such as unwanted email communication. For example, many online retailers collect email addresses to send order-related information and subsequently use these to send email messages advertising their products and services. Moreover, malicious actors can exploit a person's email address to send messages with phishing or other scams (Shukla et al., 2024; Rauti, 2019). Even when someone explicitly opts to receive email messages from a sender, the person may still find frequent messages from that sender unwelcome.

* Corresponding author.
Email addresses: sharmin.ahmed@utah.edu (S. Ahmed), ejrader2@wisc.edu (E. Rader), sameer.patil@utah.edu (S. Patil).

https://doi.org/10.1016/j.ijhcs.2025.103599
Received 12 December 2024; Received in revised form 15 May 2025; Accepted 8 August 2025
Available online 3 December 2025

Unfortunately, avoiding or preventing unwanted email messages is inherently difficult. Laws like CAN-SPAM[1] in the United States were created to regulate commercial email messages and protect people from unsolicited email messages. CAN-SPAM mandates that commercial email messages be transparent, grants recipients the right to opt out, and imposes penalties on entities that fail to comply with these requirements. However, it does not prohibit senders from initiating unwanted contact because it requires people to opt out of receiving email messages rather than opting in (Ju et al., 2021).

In addition to their communicative purposes, email addresses are used for authentication because they are typically tied to people's identities (Gruss et al., 2018). In fact, many services use email addresses as usernames for user accounts. As a result, email addresses can be used to identify people and link their records across multiple systems or platforms to profile and track their activities (Chen, 2023). Undesirable disclosure of email addresses thus makes people reachable or identifiable by parties by whom they may not want to be contacted or identified. Consequently, people may be reluctant to provide their email addresses to persons, organizations, or systems they do not trust.

People often face situations in which they are asked for an email address, even when they are uncomfortable providing one. People may deal with such situations by providing secondary or throwaway email addresses instead of disclosing the primary email addresses associated with their personal or professional identities (Kang et al., 2013; Rader and Munasinghe, 2019). Alternatively, people may provide email addresses that are not theirs, often by crafting one on the spot. Preventing people from claiming someone else's email address as their own requires that anyone providing an email address confirm ownership of that email address through appropriate verification mechanisms, such as a code or a link sent to the email address. The person providing the email address must subsequently provide the code or click the link before that email address is associated with that person. However, to reduce the friction and effort of verification, many services enable partial access to functionality without verification or skip the verification step altogether (Sudhodanan and Paverd, 2022). For instance, Kubicek et al. (2024) found that only 42.4 % of websites in their sample withheld access before verifying ownership of the email address, and 24.8 % sent only an email message confirming the creation of an account associated with the email address.

As an example, consider the following scenario:

> While creating a profile on a dating site, Alice is concerned about her privacy. Therefore, she decides to create the profile using a made-up email address. Instead of her email address, `alice@email.com`, she registers an account on the site with the email address `alicia@email.com`. The site does not request additional verification from Alice to confirm that she owns the email address alicia@email.com. Unbeknownst to Alice, the email address she created belongs to Alicia, who soon starts receiving a flood of email messages from the dating site intended for Alice. The messages Alicia receives include Alice's personal information, such as dating activity, profile updates, messages from potential matches, and personalized recommendations.
>
> Alicia attempts to unsubscribe from the email messages sent by the dating site, but is unable to do so without logging into the account, which she cannot do since she does not know the password. Frustrated, Alicia seeks assistance from the customer service of the dating site. However, the customer service representative refuses to help without verifying the account through the phone number associated with it. Alicia cannot verify the account because the phone number on file is not hers. Attempting to log in to the site fails because of the same issue, leaving Alicia unable to resolve the situation.
>
> Alicia's husband Bob notices the email messages from the dating site, fueling his suspicions about Alicia's faithfulness. Alicia's inability to control the situation intensifies the misunderstanding and creates strain in her marriage. Meanwhile, Alice is unaware of Alicia's situation and continues to use the site for dating activities.

We refer to an alternate email address crafted to avoid disclosing one's email address as a 'made-up email address.' As the above scenario illustrates, a made-up email address may be an active one belonging to another person. In such cases, if personal information about the person who provided the made-up email address is sent via email, it is received by the owner of that email address without the provider of the made-up email address being aware of the information disclosure (Rader and Munasinghe, 2019). Thus, providing a made-up email address to avoid the privacy risks of disclosing one's email address to an untrusted entity could ironically lead to other kinds of privacy invasion. Made-up email addresses hold privacy implications for the owners of these email addresses as well. Email messages sent to a made-up email address breach the communication boundaries of the owner of that email address and create information overload for that person.

People may engage in other practices similar to providing made-up email addresses. For instance, people often enter incorrect contact information and personal detail in online forms to protect their personal information from potential breaches and third-party sharing (Captain, 2024). Similarly, people may provide made-up or virtual phone numbers when they are uncomfortable disclosing their phone numbers or when they feel that giving the information is likely to result in unwanted or spam calls (McDonald et al., 2021). In cases where providing their phone numbers cannot be avoided, people may obfuscate or falsify the associated metadata (e.g., name, address, etc.) to disrupt the use of the phone numbers for tracking purposes. However, findings from the phone context may not fully generalize to email because of the differences between how people and businesses use phone numbers and email addresses for communication (Ackerman et al., 1999). Focusing on the practice of providing a made-up email address can illuminate the individually and socially motivated tensions that are often overlooked in broader studies of avoidance or filtering. Yet, researchers have not yet studied why people provide made-up email addresses, despite the privacy risks to themselves and others, nor how people craft these addresses. We addressed this gap with the following research questions:

- **RQ1:** Why do people provide made-up email addresses instead of their own?
- **RQ2:** What patterns do people use to compose made-up email addresses?

To answer the above questions, we conducted in-person semi-structured interviews with 20 individuals, all of whom had provided made-up email addresses as indicated by their responses to a pre-study screening questionnaire. In addition to asking the participants to describe their experiences with made-up email addresses, the interview covered three specific scenarios in which someone might provide a made-up email address. Based on inductive thematic qualitative analysis of the interview transcripts inspired by grounded theory (Saldaña, 2021), we uncovered misalignment between user expectations of email privacy and requests for email addresses. We found that people provide made-up email addresses as a workaround to avoid information overload from unwanted email messages and to preserve privacy without violating situational norms.

Our findings characterize the practice of providing made-up email addresses as a *strategic* response necessitated by the challenges inherent to email as a sociotechnical system. We apply the insight to characterize made-up email addresses as a privacy-oriented boundary management mechanism (Petronio, 2002). In addition, we offer suggestions for design improvements and public policy interventions to minimize requests for email addresses and to avoid the privacy issues and information overload

[1] https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business.

caused by misdirected email messages that result from the practice of providing made-up email addresses.

In the following sections, we first review related literature in the email domain. Next, we describe our methodological approach and provide information on our sample and data analysis. We then present the empirical findings that answer the above research questions and discuss how these findings relate to several theories of human behavior. We proceed to highlight the implications of our work for addressing the privacy issues associated with made-up email addresses and conclude with remarks calling for a systemic sociotechnical approach to address the issues that lead people to provide made-up email addresses.

2. Related work

Our work builds on the literature on information overload in the email context, marketing carried out via email, and privacy concerns related to email communication. To contextualize the challenges and motivations behind the use of made-up email addresses, we review the salient related work in each of these domains.

2.1. Information overload from email

Although email plays a significant role in modern society, its ubiquity introduces complexities. Whittaker and Sidner (1996) used the term 'email overload' to describe the strain people experience because of the sheer volume of email messages. These challenges are exacerbated by the evolution of email from a mere communication tool into a "habitat" for personal information management, coordination, and collaboration (Ducheneaut and Bellotti, 2001). In a study conducted nearly 20 years after that of Whittaker and Sidner (1996), Grevet et al. (2014) noted that email overload remains a persistent issue. The overload results from not just the volume of incoming email messages but also the substantial cognitive effort required to navigate and organize them (Jones and Kelly, 2018) and determine the relevant action(s) to process each message (Grevet et al., 2014). Akbar et al. (2019) have demonstrated that frequent interruptions from email messages can not only induce emotional stress but also provoke expressions of anger in email responses. More recent studies in the work context have highlighted that the increased cognitive load resulting from high email volumes lowers productivity and job satisfaction (Tarafdar et al., 2023; Letmathe and Noll, 2024).

In addition to the negative impact on productivity and affect, email overload can pose security risks (Shukla et al., 2024). For instance, Shukla et al. (2024) found that attackers can subscribe people's email addresses to thousands of mass mailing lists, flooding their Inboxes to make it difficult to identify legitimate email messages among the deluge. The difficulties in separating legitimate and unwanted email messages can subsequently be exploited to carry out other attacks, such as phishing, spreading malware, etc. (Shukla et al., 2024).

Regardless of the source, unwanted email messages compound the challenges of email overload and degrade the overall user experience of email management. Managing an Inbox full of unwanted email messages requires a person to take explicit actions, such as deleting, filtering, marking as spam, unsubscribing, etc. (Micheaux, 2011; Sergeeva et al., 2023). Dev et al. (2020) found that users are often frustrated by confusing multi-step processes and obscure options that many companies deliberately employ to make it difficult for users to unsubscribe from unwanted email messages. Managing email with filters is similarly challenging because improper filtering could result in false positives that prevent legitimate email messages from reaching the Inbox (Bhagyavati et al., 2004).

To deal with email overload, people may limit the volume of incoming email by avoiding the disclosure of their email addresses in certain situations and giving out made-up email addresses instead. Our research aims to shed light on the motivations behind the practice and the situations in which people engage in it.

2.2. Marketing via email

The volume of Business-to-Consumer (B2C) email, such as coupons, deals, receipts, and event notifications, has increased significantly in recent years. Consequently, dealing with such email plays an increasingly larger role in email management (Bentley et al., 2017). As far back as 2017, 92 % of American adults received B2C email messages, and 65 % actively engaged with these messages within two weeks (Daskalova et al., 2017). Sergeeva et al. (2023) found that companies employ various persuasive tactics to encourage impulsive subscriptions to their mailing lists, and people often regret subscribing due to the subsequent influx of promotional email messages sent to the mailing lists. The issue of unwanted promotional email messages extends to academic contexts as well (Wood and Krasowski, 2020; Hartemo, 2021).

Researchers have found that people express negative emotions toward frequent (Cases et al., 2010) and personalized (Boerman et al., 2021; Maseeh et al., 2021) marketing email messages. In addition, people report being concerned about commercial entities sharing their email addresses with third parties (Boerman et al., 2021; Sergeeva et al., 2023). Therefore, our research explicitly included such situations to investigate their connection to the practice of providing made-up email addresses.

2.3. Privacy concerns related to email

Englehardt et al. (2018) found that nearly a third of the email messages received through mailing lists contain embedded content that transmits the recipient's email address to third parties, thus raising concerns about privacy and control over personal information. Relatedly, Senol et al. (2022) discovered that email addresses entered by people when filling out online forms may be transmitted to third party tracking, marketing, and analytics services even before the form is submitted. The harvesting of email addresses in such ways highlights that if people disclose their email addresses, it often increases the likelihood that the email addresses will be used for sending them commercial email messages and/or tracking their real-world activities (Chen, 2023).

Given the various risks of disclosing email addresses, people protect the disclosure of their email addresses through a variety of practices, such as using multiple email accounts, restricting the disclosure of email addresses to specific contexts, etc. (Kang et al., 2013). While Rader and Munasinghe (2019) pointed out that providing a made-up email address is an additional protective practice, they did not delve into the motivations, circumstances, and methods involved in this practice. Moreover, researchers have not yet explored whether individuals who engage in the practice of providing made-up email addresses recognize the impact on the owners of these email addresses. Our work addresses this gap through an exploration focused on an in-depth understanding of the practice and considers the implications for owners of made-up email addresses.

3. Method

To answer the research questions listed in Section 1, we used a qualitative methodological approach, as it is ideally suited for initial exploratory investigations that aim to capture in-depth, nuanced descriptions of motivations and contextual factors underlying specific practices (Alase, 2017). Specifically, we developed a semi-structured interview protocol informed by the literature on email management and privacy management. The protocol covered email in general, without privileging work or personal email. We used the protocol to interview 20 individuals who indicated that they had made up an email address when asked to provide one. In the subsections below, we present the study protocol, describe the recruitment and study procedures, characterize the sample, explain the data analysis procedures, and point out a few limitations.

3.1. Semi-structured interview protocol

The initial part of the semi-structured interview protocol comprised general questions about email use to gain insight into email management preferences and practices. Studying the practice of providing a made-up email address requires understanding how it is embedded within the larger context of email. Since behavior related to email management is relative to the unique context of a person's experiences with email, we asked participants to show us their Inboxes as in other research on email use (Grevet et al., 2014). We used the Inbox as a reflective prompt to help recall specific examples of messages that illustrate email management and practices related to email privacy. Since we asked about the most-used email address, we expected that participants would show us the Inboxes for those email accounts. However, participants were free to show us the Inboxes of any of their email accounts. We included follow-up questions on the organization of the email account and challenges in managing email messages. The approach enabled us to pose questions about thoughts and practices related to handling real-world email messages, thus collecting more accurate and authentic data.

The next part of the interview covered personal experiences of providing made-up email addresses. The questions asked participants to describe the situations and discuss the motivations behind providing made-up email addresses. To uncover the mental models involved in crafting a made-up email address, we asked participants to create made-up email addresses by imagining themselves in the same situations and to explain the thought process used to construct the email addresses.

The last part of the interview asked participants to role-play three scenarios involving the disclosure of email addresses:

- **Shopping at a Store:** Imagine that you are out shopping at a store. When you are checking out at the cash register, the cashier asks for your email address so the store can send you an electronic receipt.
- **Buying a Car at a Car Dealership:** Imagine that you are considering buying a new car and have been going to various dealerships to view and test drive various models. After showing you the available vehicles, the salesperson asks for your email address.
- **Encountering a Paywall on a Streaming Service:** Imagine that you are using a new online streaming service. After streaming a few videos, you encounter a paywall that requires you to create an account on the platform for a paid subscription to the service. You can get a one-month free trial before the platform asks for your credit card information. When creating your account, you are asked to provide your name and email address.

To identify suitable scenarios, we conducted brainstorming sessions in which the research team examined example email messages received by the authors and generated ideas about situations in which someone might provide a made-up email address. The above three brief scenarios were deemed the most plausible in an informal pilot of candidate scenarios constructed from the ideas generated in the brainstorming sessions. We asked participants which email address they would provide in each scenario and why. Including the scenarios in the interview protocol enabled us to collect data on a common set of situations, facilitating comparisons across participants.

The complete interview protocol is available in Appendix B.

3.2. Recruitment and study procedures

We recruited participants through a study advertisement titled 'Managing Unwanted Email.' We posted the advertisement to a community-focused pool of participants affiliated with a large public university in the United States. The study was open to adult knowledge workers who were not undergraduate students. We chose to recruit knowledge workers and exclude undergraduate students because, compared to typical students, knowledge workers use email for workplace communication and coordination as well as for personal online tasks, which could give us insight into email practices across both work and personal contexts (Grevet et al., 2014). The recruitment criteria facilitated the generation of insight that more accurately reflects broader email use and privacy concerns.

To confirm eligibility for the study and enable us to recruit a diverse sample, the advertisement directed those interested in participating to a brief screening questionnaire (see Appendix A). Those who answered the screening questionnaire provided their experiences with made-up email addresses by responding to the following statements:

- I have made up an email address on the spot to avoid giving out my email address.
- I have given out a slightly different version of my email address.
- I have given out a random email address instead of mine.
- I have entered the shortest possible combination of characters that could pass as a valid email address when entering my email address online.
- I have refused to provide my email address when someone asked for it.

Since we were interested in studying practices connected to providing made-up email addresses, we used the responses to the above statements to exclude those who did not report having provided a made-up email address. To avoid bias, we additionally excluded anyone who had previously participated in other research studies conducted by our research lab.

After filtering responses to the screening questionnaire based on the recruitment criteria described above, we invited a subset of the eligible individuals to participate in the interview study. We selected the subset by prioritizing demographic diversity in the sample. We informed those we invited to participate that the interview would involve logging into their email accounts and showing the interviewer their Inboxes. We requested that participants bring their own devices to log in to their email accounts during the interview, but provided a guest laptop for those who were unable to do so.

We instructed the participants to delete or hide email messages in their primary email accounts before the interview if they did not want to show or discuss those messages during the interview. The study protocol ensured that the participants decided which email messages to discuss or use as examples in response to questions. Therefore, only those email messages that the participants chose to discuss are included in our data. At the start of the interview, we reminded the participants that they could refuse to answer any questions or withdraw from the study at any time without forfeiting the reward for study participation. All participants chose to show us their Inboxes during the interview, and none withdrew from the study or refused to answer any questions.

The interviews lasted between 28 and 65 min, with a mean of 45 min. We audio-recorded the interview sessions. At the end, we provided the participants with additional information about the research to familiarize them with the issue of misdirected email that can result from made-up email addresses. Each participant received a $30 Amazon.com gift certificate as a reward for the study participation.

When designing and conducting the study, we explicitly addressed ethical considerations. All participants received information about the study before the interview and provided informed consent to participate. The screening questionnaire, the study invitation, and the consent form informed potential participants that the study involved showing their email Inboxes to the interviewer and instructed them to delete or hide any sensitive email messages before participation. To protect participant privacy, we did not ask for specifics regarding any email messages and did not capture device screens. We ensured that anyone who used the guest laptop logged out of email accounts at the end of the interview and cleared the browser history, cookies, and cache of the guest laptop immediately after the interview. Before analysis, we assigned each participant a non-identifiable numeric ID and anonymized personally identifiable information (e.g., email addresses, names, etc.) in the interview responses. All study procedures were reviewed and approved by the Institutional Review Boards (IRBs) of our universities.

Table 1
Demographics of the study participants.

Participant ID	Gender	Age group (*years*)
P01	Man	41–45
P02	Woman	36–40
P03	Woman	31–35
P04	Man	26–30
P05	Man	41–45
P06	Woman	31–35
P07	Man	31–35
P08	Woman	26–30
P09	Woman	26–30
P10	Man	21–25
P11	Woman	31–35
P12	Woman	21–25
P13	Woman	31–35
P14	Woman	31–35
P15	Woman	21–25
P16	Man	31–35
P17	Woman	21–25
P18	Woman	26–30
P19	Woman	41–45
P20	Man	26–30

3.3. Sample

We used the semi-structured interview protocol described above to conduct interviews in late November and early December 2019. We reached saturation (Guest et al., 2006) after interviewing 20 participants. Table 1 provides the demographics of the sample. As shown in Table 1, the sample included seven men and 13 women ranging in age from early 20s to mid-40s. All participants worked in roles generally considered as knowledge work. Over half of the participants were connected to the university as current or former employees or graduate students in disciplines unrelated to our research topic. Four participants were graduate students or visiting scholars, and three were temporary instructors. Five others were university staff who worked in educational program development or office support. Three participants worked for the state government; one was a software developer; and another was a microscope technician. The remaining three participants did not provide their occupations.

3.4. Data analysis

We augmented the transcripts of the interviews with notes taken by the interviewer during the study sessions and subsequently anonymized the transcripts. We analyzed the transcripts in several rounds of inductive thematic analysis inspired by grounded theory (Saldaña, 2021). The first author coded the transcripts, guided by the other two authors. As the coding progressed, all authors met regularly to discuss emergent themes and refine codes.

The first round of coding involved structural coding to annotate sections of the interview transcript and open coding to mark salient topics discussed by the participants. We explicitly coded participant descriptions of various email management practices, including the use of made-up email addresses and other protective measures. When coding, we paid attention to the underlying motivations behind the reported practices, such as reducing information overload, protecting privacy, enhancing security, etc.

The second round of coding focused on grouping the lower-level codes into higher-level themes. After settling on a set of higher-level themes, we double-checked the coding to ensure consistency of the codes associated with each theme and to identify patterns that we might have missed or counterexamples that could refute the interpretation captured in the codes. We then categorized recurring themes according to similarities across the participants. As the coding progressed, we discussed the relationship between the themes and the concepts and findings from the literature on information overload, email management, and interaction boundaries. For example, the various motivations marked during the open coding were combined into codes such as 'managing information overload,' 'regulating communication boundaries,' etc.

3.5. Limitations

Our study used a small convenience sample, with purposive sampling to recruit individuals who had engaged in proactive practices related to avoiding the disclosure of their email addresses. However, our sample size is typical for exploratory qualitative research that relies on saturation to determine when to stop collecting data (Guest et al., 2006; Marshall et al., 2013). We deliberately excluded those whose approach to dealing with unwanted email messages was to take action only *after* an email message is received. The participants in our study were knowledge workers from the community surrounding a large public university, so their email use and email address disclosure preferences and practices may differ from those of individuals who are not knowledge workers. Although our sample cannot be considered representative, the themes derived from our data and the implications based on these themes have the potential for broad applicability because of the ubiquity of email and the variety of purposes for which email addresses are used. However, verifying the extent to which the findings generalize to other populations requires further research.

4. Findings

We analyzed the interview data to examine why people provide made-up email addresses (RQ1) and which composition patterns they use to craft these addresses (RQ2). The analysis identified several situations in which the participants provided made-up email addresses. The practice was driven by self-focused and social motivations (*RQ1*). We found that the participants composed made-up email addresses based on their mental models of the form expected of a valid email address (*RQ2*). We additionally uncovered that the decision to use a made-up email address was often influenced by various threat models underlying the perceived consequences of providing the email address (*RQ1*). The participants justified the appropriateness of the decision by framing it as a proactive defense mechanism against online threats and information overload (*RQ1*). In the subsections below, we cover each of the above aspects in detail, supported by illustrative participant quotes.[2]

4.1. Disclosure contexts

We observed several commonalities in the situations in which the participants opted to provide made-up email addresses and in the motivations underlying the practice. For example, when signing up for an offer to receive free product samples, P18 provided a made-up email address by slightly altering her email address:

> "It was a cosmetic shop, and they were conducting a survey outside their store. They were giving out free samples of their cosmetics and asked us to fill out the survey to get those free samples. At the end, the survey asked for my email address and cell phone number. So I put an email address and a cell phone number [that were] slightly different [from mine] because I did not want to give the real information." — P18 (Woman, Age: 26–30)

In the above instance, P18's actions were driven primarily by privacy concerns and a desire to avoid receiving promotional email messages. Some other participants similarly reported avoiding the disclosure of their email addresses if the requester seemed untrustworthy or if they wished to remain anonymous when providing confidential feedback or filing complaints, especially when they did not need to verify the email address provided. For example, P05 described an instance of providing a

[2] We have lightly edited the quotes to correct typos and grammar while preserving the semantics.

Table 2
Reasons for providing made-up email addresses in various situations.

Situations	Reasons
Registration for coupons or samples	Maintaining communication boundaries; Preventing spam and information overload
Participation in campaigns or research	Minimizing participation effort; Maintaining anonymity
Registration and information input on online platforms	Protecting personally identifiable data; Maintaining anonymity
Interaction with untrustworthy requesters	Protecting personally identifiable data

made-up email address when stating a potentially controversial opinion on a discussion forum that did not verify email addresses:

> "I wanted to get my point across without alienating people. […] It just said enter an email address. It did not verify it, so I put something close to my email address." — P05 (Man, Age: 41–45)

In the above situation, P05 avoided using a random string of characters for the made-up email address to ensure that it appeared credible and was not considered as having been generated by a bot. He shared that he uses the shortest possible string of characters to save effort when composing made-up email addresses for participating in research or surveys. By using the shortest possible string, P05 minimized inconvenience and effort while also protecting his privacy by avoiding the disclosure of his email address.

Table 2 provides an overview of the different disclosure contexts and the main reasons the participants stated for providing made-up email addresses in those contexts. The contexts include a variety of situations in which the participants were asked to register for online services and provide input, such as reviews, feedback, etc. Providing made-up email addresses was especially common when the participants interacted with services that did not require verification of the provided email address and/or those that the participants deemed untrustworthy. The various reasons the participants mentioned for providing made-up email addresses involved the desire to maintain privacy by staying anonymous, avoiding the disclosure of personally identifiable information, and managing incoming communication.

4.2. Self-focused motivations

Our analysis revealed that disclosure of email addresses raised concerns about the challenges of information overload and privacy management. These self-focused concerns led the participants to use made-up email addresses to control who could communicate with them by email. We describe these self-focused motivations, covering how the participants leveraged made-up email addresses to regulate communication boundaries, manage information overload, and balance the risks and benefits of sharing their email addresses.

4.2.1. Regulating communication boundaries

The participants strategically used made-up email addresses as a defense mechanism to counteract persistent intrusion from unwanted email and to maintain communication boundaries in their email interactions. For example, P11 explained that she provided a made-up email address because she did not want to receive unwanted email messages:

> "Because I do not want them [unwanted email messages] in my Inbox, basically. If it is a product that I really do not have any interest in…I just scribble something down [as an email address]." — P11 (Woman, Age: 31–35)

Using a made-up email address in the above case helped P11 protect herself from the intrusion resulting from unwanted marketing email messages. Other participants similarly articulated that providing a made-up email address was a practical way to assert their right to privacy:

> "I think people have a right to privacy. I do not have to distribute my information to everyone. I would give an email address that is obviously fake[3] so that they [the requesters] can get the message [that I do not want to disclose my email address]." — P10 (Man, Age: 21–25)

When trying new apps, P16 provided made-up email addresses unless an app was from a reputable company that he believed was unlikely to share or sell his personal information:

> "If it is a well-known company like Nintendo, I would not do that [provide a made-up email address]. They will not sell my information. At least I think so. But if it is a company I do not know, like an app that I have never heard of but I am interested in trying, then I will download the app and sign up [for an account] with a fake email address." — P16 (Man, Age: 31–35)

The above examples illustrate that the participants used made-up email addresses to reinforce their communication boundaries and maintain privacy by attempting to limit the dissemination of their personal information. Their practice of using made-up email addresses for these purposes reflects their awareness of the risks associated with sharing email addresses, particularly given the difficulty of knowing whether the entities collecting their information might sell or misuse it.

4.2.2. Managing information overload

When discussing the state of their Inboxes, the participants expressed frustration that their Inboxes frequently became cluttered with marketing email messages. P19 experienced an excessive volume of email messages after providing her email address for subscriptions:

> "I subscribed to something and gave them my email address, then I got bombarded like crazy with email messages." — P19 (Woman, Age: 41–45)

P05 expressed similar frustration about stores requesting his email address to sign up for services, leading to a constant stream of unwanted email messages that required him to go through the tedious process of unsubscribing:

> "I was shopping, and every store wanted me to sign up for an account or a credit card. I am getting constant emails from these stores where I shopped only once, so I had to do unsubscribe, unsubscribe, unsubscribe." — P05 (Man, Age: 41–45)

P09 mentioned that unsubscribe links did not work about a quarter of the time. Even when unsubscribe links worked, P09 and P11 felt that they continued to receive the email messages despite having unsubscribed:

> "I was getting so many weird emails. I had no clue when I subscribed to those. I tried the unsubscribe options, but they did not work most

[3] Although most participants characterized the email addresses they made up as "fake," not all email addresses they made up were non-existent. It was likely that several of the made-up email addresses were working email addresses belonging to someone else. Although we have used the term 'made-up email addresses' to refer to such email addresses (see Section 1), we have preserved the word 'fake' when quoting the participants if a participant used it to describe made-up email addresses.

of the time. Even though [it said] I unsubscribed, I still get those emails." — P09 (Woman, Age: 26–30)

"Although I unsubscribed several times, it never unsubscribed me. I contacted them and said, 'Look. Screenshot. Unsubscribe. What is going on? I never provided my email address to you guys. I do not know where you came from.' The people on the other end said, 'That does not make any sense. The unsubscribe should work.' " — P11 (Woman, Age: 31–35)

When attempting to deal with information overload by unsubscribing from unwanted email, the participants reported numerous difficulties, such as cumbersome processes, non-responsive systems, deceptive design patterns, non-working unsubscribe links, etc. As a result, the efforts to unsubscribe were often unsuccessful, and the participants continued to receive the unwanted email messages. The experiences of the participants in our study echo those reported in prior work on the user experience of unsubscribing (Dev et al., 2020). Because of these experiences of receiving unwanted email messages that were challenging to stop, the participants subsequently adopted the practice of providing made-up email addresses as a strategic response to reduce Inbox clutter.

4.2.3. Balancing risks and benefits

When deciding to provide a made-up email address, the participants weighed the benefits of providing their email addresses against the risks. P05 explained that perceived benefits influence his decision regarding whether to disclose his email address. P05 noted that online surveys often request email addresses without a legitimate reason, such as delivering a gift certificate:

"If there is no reason, like I am not going to get an Amazon gift certificate or something like that, why do you need my email address?" — P05 (Man, Age: 41–45)

In such cases, the lack of justification influenced him to use the shortest possible string as his email address. P07 reported that he discloses his email address only when the requesting parties are of significant interest to him or present a personally relevant promotional offer:

"I provide my email address only for things that I really care about." — P07 (Man, Age: 31–35)

Interestingly, P07 believed that it was common to use made-up email addresses and assumed that it caused no harm:

"I assume that the whole world gives out some kind of fake email address." — P07 (Man, Age: 31–35)

When presented with the role-playing scenario of buying a car at a car dealership (see Section 3), most participants indicated that visiting a car dealership suggests an interest in purchasing a vehicle. The participants stated that they would not provide a made-up email address in such a situation because the request for an email address occurred in the context of a self-initiated interaction:

"If it is a car-buying experience, I am initiating the interaction. So I am actively looking for a car…In this case, I am giving my email address to somebody who is being helpful to me." — P11 (Woman, Age: 31–35)

Anticipation about future communication played a major role in deciding which email address to provide:

"It depends on why they want my email address. If they want my email address so I can communicate with them directly about a purchase I want to make, I would give them [the email address for] my personal email account. However, if they just wanted to sign me up for an email list, I would decline and not give them my email address." — P12 (Woman, Age: 21–25)

When the participants believed that email communication was necessary for accomplishing their goals, they were comfortable providing their email addresses. In the absence of such expectations, the participants indicated they would either decline to provide their email addresses or provide made-up ones instead. For example, P05 stated that he would provide a made-up email address when interacting with car dealerships because of the negative experience of being unable to unsubscribe from email messages from a car dealership to which he had provided his email address in the past:

"The car dealership where I bought my car…I swear I have tried to unsubscribe because it is in another state. I could not buy another car from them [now], but they still email me. […] Once they have your email address, it is forever." — P05 (Man, Age: 41–45)

4.3. Social motivations

In addition to self-focused motivations, the participants were influenced by social expectations when deciding whether to provide a made-up email address when someone asked for an email address. Made-up email addresses enabled the participants to conform to social norms regarding expected responses to such requests without compromising their privacy. At the same time, the participants needed to cope with the anxiety of the deception being discovered and the guilt of not providing accurate information.

4.3.1. Conforming to social norms

Many participants expressed that they felt compelled to provide an email address when asked, particularly during in-person interactions. The feeling was driven by the social expectation that individuals share contact information when requested. The participants found it challenging to decline the requests because they worried that a refusal could be perceived as unfriendly, uncooperative, or socially inappropriate (Johnson et al., 2004). For example, when role-playing the scenario of shopping at a store, P20 stressed that he is careful about not appearing mean when declining to provide his email address:

"I am conscious of trying not to be angry or mean about [refusing to provide my email address], just saying, 'No. Thanks.' " — P20 (Man, Age: 26–30)

Instead of declining, many participants chose to provide a made-up email address. For instance, when P12 was asked why she gave out a made-up email address instead of refusing to provide an email address, she noted that it was because she felt uncomfortable declining the request:

"I felt awkward saying no, even though I did not want to give my email address…I am not very good at saying flat out no to people." — P12 (Woman, Age: 21–25)

Even those who declined initially reported resorting to providing made-up email addresses when faced with persistent requests. For example, when asked what he would do if asked persistently for his email address, P20 said:

"I would probably first try again to say, 'No, I am not going to give you one.' Then, I would probably say, 'All right. If you make me give you one, I am going to give you a fake email address.' " — P20 (Man, Age: 26–30)

Using a made-up email address in the above situation allowed P20 to uphold the appearance of conforming to social norms without exposing himself to future unwanted email messages. In such cases, some participants reported that they tried to protect their email addresses by writing them in an illegible manner to make them difficult to read. A few participants mentioned that they sometimes provide old, inactive email addresses instead of made-up ones.

Made-up email addresses served as butler lies that helped the participants maintain social courtesy without compromising personal privacy (Hancock et al., 2009). To help preserve the butler lies, the participants crafted made-up email addresses closely resembling theirs. The

Table 3
The composition patterns employed by the participants when creating made-up email addresses, illustrated with fictitious example email addresses.

Patterns	Participant's email addresses	Made-up email addresses
Using a different domain	jane.doe@email.com	jane.doe@epost.com
Changing names to initials	janedoe@email.com	jd@email.com
Switching word order	jane.doe@email.com	doe.jane@email.com
Combining two email addresses	jane.doe@email.com, jane.work@email.com	doe.work@email.com
Adding or removing characters	jane.doe@email.com	janedoe59@email.com, jane@email.com
Using humorous or sly messages	jane.doe@email.com	strange.lady@email.com, vote.blue@2024.com
Combining random words and numbers	jane.doe@email.com	cat789@email.com, brown.cat@email.com
Using the shortest workable string	jane.doe@email.com	x@y.com
Combining random characters and numbers	jane.doe@email.com	asfas213@isw.com

participants felt that a realistic made-up email address would avoid raising suspicion about the lie. For example, P01 shared that it is important to him that a made-up email address appear genuine:

> "If I were going to engage in deception [by providing a made-up email address]…I want to do it properly. I want it to look legitimate." — P01 (Man, Age: 41–45)

P03 likewise stated the importance of providing a made-up email address that is perceived as valid:

> "I wanted to give a made-up email address which would make the person [requesting the email address] feel that it is a real email address." — P03 (Woman, Age: 31–35)

As the above quotes illustrate, the participants engaged in complex decision-making to preserve personal privacy while adhering to social expectations. Using made-up email addresses strategically helped the participants maintain the perception of conforming to social norms despite deviating from them in reality.

4.3.2. Navigating anxiety and guilt

Deviating from social norms while maintaining the appearance of conforming to them made some participants feel anxious and guilty about providing made-up email addresses. For instance, when providing a made-up email address, P16 was concerned about the possibility of being caught in a lie:

> "[When providing a made-up email address] in person, they can catch you if they check [the provided made-up email address]. That makes me fear that they are going to prove that I am lying and causes anxiety." — P16 (Man, Age: 31–35)

The conflict between preserving privacy and maintaining socially appropriate behavior was evident in the various mechanisms the participants used to compose made-up email addresses. P19 expressed concerns about providing a random email address, noting that she would feel embarrassed if she could not remember it if she were asked to repeat what she provided:

> "I feel like a random email address would be difficult to remember if they asked me to repeat [the made-up email address I provided]. I would have to say, 'I do not remember.'" — P19 (Woman, Age: 41–45)

P16 expressed the discomfort he would feel if caught providing a made-up email address, making him more mindful when crafting one:

> "I imagine they would probably say, 'Hey, you gave me a fake one. Give me a real email address.' […] I want to avoid it at all costs." — P16 (Man, Age: 31–35)

The feelings of discomfort experienced by the participants illustrate that they valued the privacy protection achieved by providing a made-up email address despite feeling guilty about it. The feelings of anxiety and guilt for providing a made-up email address were less pronounced in online situations because there is no face-to-face interaction:

> "I feel a lot less guilty about giving out a fake email address online because the person who requested [my email address] is not in front of me." — P18 (Woman, Age: 26–30)

4.4. Mental models

As we noted in Section 4.3.2, the participants often expressed that made-up addresses needed to appear realistic. The participants believed that using made-up email addresses that appear realistic would avoid personal repercussions and circumvent verification processes. We delved deeper into investigating practices related to the composition of made-up email addresses by asking the participants about the made-up email addresses they had provided. In case a participant could not recall the specifics, we asked the person to craft made-up email addresses during the interview.

The made-up email addresses the participants shared or crafted followed a few notable patterns that mostly involved modifications to their own email addresses. Analyzing the properties of the made-up email addresses the participants shared or crafted during the interview helped us identify the mental models of the participants regarding what email addresses they consider realistic. The mental models often relied on assumptions about the commonness of their email addresses and/or names. We first present our analysis of the formats of the made-up email addresses the participants shared or crafted, followed by the reflections of the participants on the impact of the chosen formats on themselves and others.

4.4.1. Properties of made-up email addresses

The fictitious examples in Table 3 illustrate the various composition patterns the participants employed in the made-up email addresses they shared or crafted during the interviews. In many cases, the made-up email addresses were based on their own email addresses or names. Some participants crafted made-up email addresses by modifying their email addresses based on the assumption that they were highly uncommon, with little overlap with the email addresses of other people:

> "I think that my email address is obscure enough that other people do not have one similar to mine. My email address does not hold meaning for anybody but me, and I assume that nobody would use a similar email address." — P17 (Woman, Age: 21–25)

When modifying their email addresses to create made-up email addresses, some participants changed the domains in their email addresses, such as changing from `jane.doe@email.com` to `jane.doe@epost.com`.

Others used initials to reconstruct janedoe@email.com as jd@email.com or switched the order of the first and last names, as with modifying jane.doe@email.com to doe.jane@email.com. Another common approach was combining multiple email addresses, such as merging jane.doe@email.com and jane.work@email.com to form doe.work@email.com. Most participants reported modifying their email addresses by adding or removing characters to create made-up email addresses, as illustrated by jane.doe@email.com being modified to construct janedoe59@email.com or jane@email.com.

Sometimes, the participants composed made-up email addresses unrelated to their names or email addresses. In such cases, the participants reported creating made-up email addresses by concatenating unrelated familiar words that they could remember (e.g., brown.cat@email.com) or by creating humorous or sly messages (e.g., vote.blue@2024.com). Several participants used the shortest workable string (e.g., x@y.com) or a combination of random characters (e.g., asfas213@isw.com).

4.4.2. Personal repercussions

The participants adjusted the patterns they used to craft made-up email addresses based on their assessments of potential personal repercussions. As mentioned above (see Section 4.3), the desire to avoid awkwardness and discomfort during in-person interactions led the participants to compose made-up email addresses that they believed the requester would deem acceptable. As a result, it was more common for made-up email addresses provided during in-person interactions to be modified forms of their email addresses.

In contrast, the participants believed that negative personal repercussions were less likely in online settings. Therefore, when composing made-up email addresses in online settings, the participants were more likely to use patterns with short and/or random combinations of words, characters, and numbers, without regard for whether the resulting made-up email addresses appeared legitimate to the requesting entity. For example, in the scenario of providing an email address to remove a paywall on a streaming service that did not verify email addresses, P12 said:

> "I will use just random words and letters [when composing a made-up email address]." — P12 (Woman, Age: 21–25)

At the same time, the participants needed to ensure that the made-up email addresses they provided in online forms were in a format that met the technical specifications for valid email addresses:

> "You *have to* put in an email address [in the online form] to advance to the next step. So you must pass that test [that the provided email address is in a valid format]. I am like, 'I do not want to put my email address in, so I will give them something that checks the box [by passing the format check].' " — P01 (Man, Age: 41–45)

4.4.3. Consequences to others

The participants believed that minimal changes to their email addresses yielded made-up email addresses that appeared valid and did not overlap with legitimate email addresses belonging to others. However, regardless of the pattern used, it is not straightforward to compose a made-up email address that is guaranteed not to belong to someone else. Several participants were aware that the made-up email addresses they provided could unintentionally belong to other people and were concerned about the consequences these individuals might experience. As P18 noted, providing made-up email addresses could result in the owners of the email addresses receiving email messages that are not meant for them.

> "Maybe there is some other person who uses an email address that is really similar to mine. […] So those email addresses that I made up could be other people's email addresses, and tons of advertising email messages could be going to them." — P18 (Woman, Age: 26–30)

To avoid such negative consequences to others, P02 avoided composing made-up email addresses using variations of her email address:

> "I feel like mine is a normal email address. So other people could have a similar email address. I hate it when I get email messages meant for other people, so I do not want to do that [to someone else]." — P02 (Woman, Age: 36–40)

Yet, when providing made-up email addresses, nine of the 20 participants disregarded the potential consequences for others. While some of them had not even imagined the possibility that the made-up email addresses they provided could belong to others, others were remorseful about having provided made-up email addresses that could have belonged to others:

> "The email address I made up probably had my name on it and probably some numbers. Not too different from my email address. I felt bad because there probably is someone with that email address since my name is pretty common." — P15 (Woman, Age: 21–25)

As the above observations highlight, when using made-up email addresses to protect privacy, the participants exhibited varying levels of awareness and concern regarding the potential negative consequences of their actions for other parties who might own the made-up email addresses. While a few participants crafted made-up email addresses carefully to avoid negatively affecting others, many did not consider the potential impact on others at all. Although some participants expressed remorse about having used made-up email addresses that could belong to other people, they continued to use such made-up email addresses nonetheless.

4.5. Threat models

We discovered that the participants were concerned with three threat models that pertain to privacy and security harms that they were trying to avoid by providing made-up email addresses. The threat models help understand the specific privacy and security issues that the participants aimed to mitigate through the use of made-up email addresses.

4.5.1. Disclosure of personally identifiable information

Some participants were concerned that providing their email addresses could lead to the disclosure of personally identifiable information since people's email addresses are often intricately linked to various pieces of personal information about them. For example, P05 worried that his email address could be used to locate his home and infer sensitive information about him:

> "Maybe some malicious person would get hold of my email address and say, 'Now we know [PARTICIPANT NAME] lives on this road, and his mother's maiden name is this and everything.' So the more obstacles I can create to prevent people from getting my personal information, like my address, the better." — P05 (Man, Age: 41–45)

Many participants indicated that they were driven to use made-up email addresses because of similar concerns about protecting the personally identifiable information linked with their email addresses.

4.5.2. Sale of email addresses

Most participants wished to avoid the use of their email addresses for commercial purposes. As P12 explained when role-playing the scenario of shopping at a store, commercial entities often ask for people's email addresses without specifying the purpose behind the request:

> "Sometimes, a cashier would not even explain why the store wants your email address." — P12 (Woman, Age: 21–25)

P16 recounted that a company to which he provided his email address likely sold it to others without his knowledge:

> "I have received a couple of phishing scams at the email address [I provided to an unknown company]. I do not know where the scams came from, but I suspect it might be from parties to whom the company sold my email address and information. I cannot do anything about it now because it is too late." — P16 (Man, Age: 31–35)

Such bad experiences made the participants reluctant to use their email addresses if they did not trust that the requesting parties would not misuse the provided email address. In such cases, the participants provided made-up email addresses to protect their email addresses from being shared with third parties. The participants did make rare exceptions for entities with whom they expected longer-term engagement:

> "If I know that I am going to have a relationship with the company regardless of whether it is going to be bad about protecting my personal information, I would throw caution to the wind and sign up with my email address. However, this does not happen too often…maybe once a year." — P16 (Man, Age: 31–35)

However, in general, the participants tended to provide commercial entities with made-up email addresses to avoid the risk of their email addresses being sold and/or used for sending them unsolicited marketing messages or scams.

4.5.3. Hacking of email accounts

Many participants believed that wide dissemination of their email addresses made it more likely that their email accounts would be hacked. P15 recounted an incident where a hacker broke into her email account:

> "My Yahoo account has been hacked a few times. One of these times, it was really embarrassing because the scammer who hacked the account sent email messages to my whole contact list. I had to write all of them saying, 'Do not open that email message I sent you because it was not me!' " — P15 (Woman, Age: 21–25)

After the incident, P15 created a separate email account specifically for purchasing purposes.

To avoid the risk of unauthorized access to their email accounts because of hacking, some participants restricted the use of their email addresses to essential activities and disclosed them only to trusted parties. For non-essential interactions, especially with unfamiliar and/or untrusted parties, some participants created separate email accounts:

> "I might want to get information from them [the party requesting the email address] at some point. But I would give them a secondary email address because I do not want to use my [primary] email address for other purposes [than the ones for which I use it], and I do not necessarily trust the website of the organization [requesting the email address]." — P06 (Woman, Age: 31–35)

The participants often provided made-up email addresses to parties they found untrustworthy to shield their email accounts from the potential threat of hacking, especially if they deemed a request for an email address to be a one-off interaction:

> "I did not trust them [the requesting entities] enough to give them my email address when I wanted to send something through just one time or to create an account that I needed to use only one time. So I used a made-up email address." — P15 (Woman, Age: 21–25)

4.6. General perceptions

We asked the participants about their thoughts on providing made-up email addresses to capture general beliefs and concerns about the acceptability of the practice. Some participants characterized the practice of providing a made-up email address as a privacy-conscious act, prioritizing control over personal information and online identity:

> "Those who provide made-up email addresses are trying to control their Internet presence and limit unwanted connections through the Internet." — P05 (Man, Age: 41–45)

> "A person who gives out a fake or bogus email address values privacy." — P13 (Woman, Age: 31–35)

Several participants described the use of made-up email addresses as a method for preventing email overload by proactively reducing Inbox clutter:

> "Someone who provides a made-up email address is a person who gets enough email messages already and does not need more." — P12 (Woman, Age: 21–25)

A few participants considered using a made-up email address as a mechanism to minimize unsolicited email and spam:

> "Someone who provides a made-up email address does not want spam." — P06 (Woman, Age: 31–35)

> "The person who gives out a fake email address is someone who is frustrated with junk email." — P10 (Man, Age: 21–25)

The participants acknowledged that providing a made-up email address is deceptive:

> "Someone who provides a made-up email address is bending the truth without the other person [requesting the email address] knowing." — P04 (Man, Age: 26–30)

Yet, many participants characterized the deception as a clever practice necessary to manipulate the information flow and navigate digital spaces discreetly without undesirable consequences:

> "A person who provides a made-up email address is stealthily declining their [of those requesting an email address] stuff. It is a polite way to say no without them [those requesting an email address] knowing that I am not interested in whatever they are selling." — P11 (Woman, Age: 31–35)

In fact, some participants assumed that providing a made-up email address is a common practice:

> "We get too many email messages. So I think it is typical for most people to think, 'What can I do not to get more email messages?' […] I bet that people do it [provide made-up email addresses] a lot." — P20 (Man, Age: 26–30)

The above perceptions portray that the participants considered the practice of providing made-up email addresses as a workaround to deal with the inadequacies of current email management and data protection mechanisms.

5. Discussion

Although the use of email for personal communication has become less common over the past decade, it remains integral for communication in professional and consumer contexts (The Radicati Group, Inc., 2023). Dealing with email overload and managing privacy continue to be core aspects of people's daily lives (Arnold et al., 2023; Usman et al., 2023; Kern et al., 2024). Yet, the technical infrastructure of email has changed little since its inception. As a result, our findings hold enduring relevance for current email-related practices despite the data being a few years old.

Email addresses are used for multiple purposes (e.g., communication, identification, authentication, etc.). As our findings demonstrate, the interplay of the multiple functions makes it challenging for people to manage information overload, regulate communication boundaries, and protect their privacy. Our findings indicate that people often use made-up email addresses as a coping mechanism to deal with these issues. To uncover the underlying mechanisms and dynamics that contribute to the use (*RQ1*) and composition (*RQ2*) of made-up email addresses as a misdirection strategy, we leverage the theoretical perspectives of communication privacy, contextual integrity, and social desirability. We additionally point out that the interdependent nature of privacy affects the potential consequences of providing made-up email addresses.

5.1. Communication privacy

We can connect the use of made-up email addresses for setting communication boundaries to Altman's (Altman, 1975) boundary regulation theory and Petronio's (Petronio, 2002) Communication Privacy Management (CPM) theory.

In the context of digital interactions, boundary regulation encompasses the practices people employ to adjust access to themselves by deciding when to share personal information and when to remain anonymous (Palen and Dourish, 2003). The participants in our study leveraged made-up email addresses to create and maintain the interaction boundaries they desired (see Section 4.2.1). Made-up email addresses helped the participants separate important and unimportant communication and prevent irrelevant content from clogging their primary Inboxes. Upon sharing their email addresses, the participants had experienced a bombardment of unwanted email messages that were difficult to unsubscribe from or manage (see Section 4.2.2). As a result, when the participants did not see any value in sharing their email addresses and wanted to avoid the potential hassles and consequences that might follow, they provided made-up email addresses (see Section 4.2.3).

CPM theory states that people believe they should have the right to regulate the dissemination of their private data (Petronio, 2002; Serewicz and Petronio, 2007). In alignment with CPM, the participants in our study believed that they should have the right to protect their privacy by providing made-up email addresses. According to CPM theory, individuals regulate the disclosure of their private information by creating communication rules based on relevant contextual factors. For instance, the participants provided made-up email addresses when they believed that the requesting parties were dubious and might misuse their email addresses and/or compromise their email accounts (see Section 4.5.3). The participants recognized that they could not ensure that the parties to whom they provided their email addresses would not misuse the information (see Section 4.5.2). Such situations in which privacy boundaries are disrupted because others do not follow the privacy expectations of the information owner are characterized in CPM theory as "boundary turbulence" (Petronio, 2002). Made-up email addresses help people prevent boundary turbulence that could result from other parties violating their expectations regarding data sharing.

Joung and Yang (2009) suggest that users should have autonomy over the email messages they receive and control over who may contact them by email. Lacking adequate means to assert such control via technical mechanisms, people regulate boundaries and manage privacy by resorting to practices such as providing made-up email addresses. The use of made-up email addresses for boundary regulation and privacy management is driven by considering a combination of personal and social factors, mental models, and threat models (see Section 4).

5.2. Contextual integrity

The participants considered the context in which they encountered a request for an email address to assess whether the request was appropriate. Therefore, we analyzed the requests and participant responses through the lens of contextual integrity (Nissenbaum, 2004). According to contextual integrity, privacy is violated when the information flow does not align with the norms and expectations of the context, which is composed of the data subject, sender, recipient, information type, and transmission principle.

Considering the contextual integrity of a request for an email address involves two key aspects:

1. Whether the *request* for an email address is contextually appropriate: The participants felt that many of the requests for their email addresses were unexpected or unjustified (see Section 4.2.3 and Section 4.5.2) and found these to be privacy-invasive. As contextual integrity explains, unexpected or unjustified requests for information are typically misaligned with contextually expected patterns of information flow and are perceived as violations of privacy (Nissenbaum, 2004). In contrast, when the participants deemed a request for an email address in a given situation to be contextually appropriate and personally beneficial, they chose to disclose their email addresses (see Section 4.2.3).
2. Whether a person's *response* to the request is contextually appropriate: Independent of whether a request for an email address was contextually appropriate, the participants were uncomfortable responding to it with outright refusal, especially when the request was made in person (see Section 4.3.1). The participants felt that declining to provide an email address deviated from the norm of maintaining harmony in interactions (Johnson et al., 2004). Providing a made-up email address enabled the participants to interact politely with a response that did not violate contextual integrity, even when they found the request contextually inappropriate.

5.3. Social desirability

Social desirability bias refers to people's tendency to answer questions with responses they imagine to be more socially acceptable in order to avoid feeling embarrassed and/or to prevent negative judgment by others (Fisher, 1993). The attention the participants paid to the perceptions and judgments of the persons requesting email addresses (see Section 4.3) indicates that the composition of made-up email addresses is influenced by social desirability bias.

When the interaction was in person, the participants composed made-up email addresses that would appear acceptable to those who requested email addresses because they felt anxious about the deception (see Section 4.4.2). Concerns about social judgment in in-person situations, linked to the social desirability bias, led the participants to provide made-up email addresses that they believed conformed to the common perceptions of legitimacy for email addresses. To avoid the embarrassment of the deception being discovered, the participants often crafted made-up email addresses similar to their own to make them easier to remember in case they were asked to repeat the information. In contrast, in online situations, the participants were far less concerned about making the made-up email addresses appear legitimate and/or memorable (see Section 4.3.2).

5.4. Interdependent privacy

One individual's privacy preferences and practices can impact the privacy of other individuals, particularly in digital contexts (Biczók and Chia, 2013). Yet, a majority of the participants in our study did not recognize or consider the interdependent privacy concerns associated with providing made-up email addresses and thought of the practice as *harmless* misdirection.

As the scenario in Section 1 illustrates, the impact of someone using a made-up email address as a mechanism to safeguard privacy can inadvertently extend to other individuals if the made-up email address is in active use by someone else. Many participants crafted made-up email addresses by simply changing the domains in their email addresses (see Table 3). For example, if a Jane Doe whose email address is `jane.doe@email.com` provides the made-up email address `jane.doe@epost.com`, then *another* Jane Doe who owns and actively uses the `jane.doe@epost.com` email address could be bombarded with email messages meant for the first Jane Doe. Unsubscribing from such misdirected email messages can present issues beyond the already cumbersome process of unsubscribing (Dev et al., 2020) because opting out may require additional verification (e.g., providing a code texted to the phone number on file) that owners of made-up email addresses cannot pass. The inability to pass the verification checks makes it infeasible for owners of made-up email addresses to dissociate themselves from the misdirected email messages, thereby exacerbating the problem. In addition to receiving misdirected email messages, owners of made-up email addresses may be implicated in the activities of those who provided the made-up email addresses. Given that email addresses are often tied to identity, owners of made-up email addresses could face reputational harm or legal repercussions due to actions performed by others without their knowledge or consent.

The interdependent privacy issues arising from the practice of providing made-up email addresses are not limited to negative consequences for the owners of made-up email addresses. Ironically, attempts to *protect* privacy by providing a made-up email address could instead *compromise* the privacy of the person who employs the strategy because email messages meant for that person are received by the owner of the made-up email address instead. The recipient could exploit personal or sensitive information included within such email messages for malicious activities, such as identity theft (Rader and Munasinghe, 2019). Even if the recipient does not use the email messages in nefarious ways, the person who provided the made-up email address may miss important communication without the person and the sender being aware of it, thus resulting in suboptimal boundary regulation and privacy management (see Section 5.1).

6. Implications

The theories and frameworks discussed in the previous section situate our findings regarding the practice of providing made-up email addresses in the broader context of email use in everyday life. The issues identified through our study make the case for solutions that respect email communication boundaries, uphold contextual integrity when requesting email addresses, and safeguard interdependent privacy connected to made-up email addresses. We apply our insight to propose actionable recommendations to enhance email interfaces, improve digital marketing practices, reform public policy, and promote more privacy-oriented use of email addresses.

6.1. Enhancing the functionality to process unwanted email

One of the main reasons the participants chose to provide made-up email addresses was their desire to avoid information overload from large volumes of unwanted email messages (see Section 4.2.2). Instead of resorting to providing made-up email addresses, users could manage information overload with existing email functionality, such as Apple's 'Hide My Email'[4] feature, which performs email address masking (i.e., automatically generating alternate email addresses linked to a given email account). Alternatively, or in addition, users could automatically segregate unwanted email messages with rule-based filtering or specialized email management tools, such as AI-driven SaneBox,[5] automation-based Clean Email,[6] etc. However, none of the existing features and tools can prevent unwanted email messages from reaching users in the first place. Handling unwanted email messages using these features and tools requires users to take actions to set up, monitor, and refine the operation and deal manually with any false positives or negatives. Moreover, many of the features and tools are available only for specific email clients or services and may require payment, thus limiting their scope. The practice of providing made-up email addresses circumvents the limitations of current features and tools, preventing unwanted email messages from reaching the intended recipient without requiring additional effort.

Enhancing the current functionality to process unwanted email could make it less compelling to use made-up email addresses as a workaround, especially in light of the negative privacy implications of the practice (see Section 5.4). For example, the existing mechanisms for automatic email categorization, such as Gmail's 'Primary,' 'Promotional,' and 'Social' tabs, could be enhanced by adding a separate category for mailing lists. A dedicated tab and/or prominent visual indicators for email messages sent to mailing lists could help users identify and process such email messages quickly. More noticeable and actionable visual indicators for unsubscribe links, annotation labels, and flagging buttons could help users handle unwanted email and reduce Inbox clutter more effectively.

Additionally, we propose that email clients include a dashboard explicitly designed to help users manage recurring unwanted email messages, such as mailing list subscriptions. The dashboard could facilitate efficient processing of unwanted email messages by providing users with an interactive visual overview of the senders and types of messages sent to their email addresses. The dashboard could include functionality to set preferences and take actions in bulk, such as batch processing email messages by sender or content, creating digests for non-essential email messages, unsubscribing from unwanted mailing lists, and tracking the outcomes of completed or failed unsubscribe attempts. If unsubscribing is unsuccessful or unavailable, future email messages of the same type could be automatically deleted. The operation could be personalized by augmenting the dashboard with privacy-preserving client-side intelligence.

6.2. Improving digital marketing via email

The participants in our study provided made-up email addresses to avoid being inundated with marketing email messages from commercial entities. More than a third of the websites included in a recent study sent marketing email messages without obtaining proper consent from the recipient (Kubicek et al., 2024). If organizations were diligent about obtaining consent and sending fewer email messages that are more meaningful and personally relevant to the recipients, users might not feel overwhelmed by the marketing messages. We recommend that users be given greater control to customize incoming marketing messages beyond simply unsubscribing or deleting them. For instance, a commercial entity could develop functional and practical mechanisms that enable users to opt in to receive email messages regarding specific products, services, events, organizations, and so on. Additionally, users should be allowed to specify the frequency at which they would like to receive marketing messages. Improving digital marketing to be more respectful of user delivery preferences could increase its effectiveness, as users are less likely to delete, filter, or ignore email messages that they choose to receive. If adopted widely across the digital marketing ecosystem, the enhancements could lead to noticeable changes, such as a significant decrease in unwanted and irrelevant email messages. Over time, the changes could eventually reduce the likelihood of people feeling the need to provide made-up email addresses to avoid marketing email messages.

6.3. Reforming privacy laws and regulations connected to email

Commercial entities increasingly use email addresses to link user identities across online and offline businesses and platforms (Chen, 2023) and may share email addresses with third parties without informing users (Kubicek et al., 2024). A lack of adequate transparency regarding how their email addresses would be used and shared with other parties led the participants to employ made-up email addresses as a privacy-protecting measure. For example, existing privacy guidelines of the Federal Trade Commission (FTC) in the United States focus on people's control over data sharing but not over who may communicate with them via email and when (Popescu and Baruh, 2013). We therefore call for reforming current privacy laws, regulations, and guidelines with specific considerations for the collection, use, and sharing of email addresses by organizations. For instance, organizations often ask for email addresses even when the information is unnecessary for the task at hand. Data protection regulations should mandate that the collection of email addresses adhere to the principle of data minimization described in the Fair Information Practice Principles (FIPPs).[7] Relatedly, regulatory agencies could establish guidelines for permissible requests for email addresses.

[4] https://support.apple.com/en-us/105078.
[5] https://www.sanebox.com.
[6] https://clean.email.
[7] https://www.fpc.gov/resources/fipps/.

The double opt-in process for verifying user-provided email addresses is not consistently implemented, despite being a fundamental security and Human-Computer Interaction (HCI) principle. To address this issue, organizations must be required to implement the double opt-in process and obtain explicit confirmation that the owner of an email address has consented to its use for the specified purposes (John and Wullf, 2024). In addition to helping detect made-up email addresses, the verification could help catch inadvertent data entry errors and protect people from the privacy risks of misdirected email messages. Moreover, policies that mandate explicit verification of the provided email address before use could help avoid negative impact on people whose email addresses are given out by others as made-up email addresses.

The participants in our study resorted to providing made-up email addresses because they found it cumbersome and, in some cases, impossible to opt out of email messages from commercial entities. These experiences underscore the need to extend regulatory protection to the use of email addresses after they are collected. In addition to requiring that organizations empower users to withdraw consent and opt out of the use of their email addresses, regulations must mandate that the opt-out and unsubscribe mechanisms be clear, simple, and functional. Importantly, opt-out mechanisms must be designed to handle requests from a person whose email address was provided by someone else as a made-up email address. Implementation of these measures can be enforced by imposing adequate penalties on those who misuse email addresses.

6.4. Promoting greater recognition of privacy risks of made-up email addresses

As highlighted in the hypothetical scenario in Section 1, the use of made-up email addresses, while a strategic attempt to protect privacy, introduces interdependent privacy risks, such as misdirected email messages and breaches of confidentiality. Yet, these risks are not always evident to people. For example, many participants in our study had not considered the full implications of providing a made-up email address that might be someone else's active email address. Our findings could make users, system designers, and policymakers more aware of the potential privacy-related consequences of made-up email addresses.

Greater consideration of the interdependent privacy risks associated with using made-up email addresses may prompt users to be more diligent about ensuring that a made-up email address does not belong to someone else or dissuade them from using made-up email addresses altogether. Recognizing that the email addresses provided by individuals may be made up could lead system designers to adapt system operations to account for this practice. For instance, system designers could implement mechanisms that automatically check whether an email address exists and verify its ownership through double opt-in (see Section 6.3). Similarly, organizations could design processes that help handle use cases in which the owner of the email address is not the person who provided that email address. Greater awareness of the practice of providing made-up email addresses could help direct regulatory attention to problematic assumptions about identity based on email addresses. For instance, using email addresses as markers of identity could be restricted by law, especially in sensitive contexts, such as those involving healthcare, financial matters, etc.

7. Conclusion

Our research on made-up email addresses sheds light on a widely adopted practice that has received little research attention. We found that providing a made-up email address is a *strategic* choice to block unwanted information flows and protect privacy. The strategic misdirection helps people maintain graceful social interactions and/or use services that could not be accessed without an email address, while avoiding undesirable disclosure of their email addresses. Yet, many who provide made-up email addresses fail to recognize that the practice could compromise their privacy and negatively impact those who happen to own these email addresses. If a made-up email address provided by one party matches an active email address of another party, the first party's actions to decrease unwanted email messages can result in increasing the unwanted email messages received by the other party. We draw on theories and literature in the domains of personal information management and usable privacy and security to contribute insight that connects made-up email addresses to the larger issue of information overload from unwanted email. Users resort to the workaround of using made-up email addresses because of the lack of usable controls to manage unwanted email and the absence of adequate regulatory mechanisms to compel companies to respect people's communication boundaries. Unwanted email is a systemic problem. Addressing the problem of unwanted email, therefore, requires sociotechnical solutions that integrate technical systems and public policy. Systemic adoption of such solutions could help stop unwanted email and ultimately obviate the need for people to rely on made-up addresses as a protective measure.

CRediT authorship contribution statement

Sharmin Ahmed: Writing – original draft, Formal analysis, Writing – review & editing, Validation, Conceptualization. **Emilee Rader:** Writing – original draft, Supervision, Project administration, Investigation, Formal analysis, Conceptualization, Writing – review & editing, Validation, Resources, Methodology, Funding acquisition, Data curation. **Sameer Patil:** Writing – review & editing, Validation, Project administration, Conceptualization, Writing – original draft, Supervision, Formal analysis.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Emilee Rader reports that financial support was provided by Michigan State University College of Communication Arts and Sciences. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

We wish to thank Anjali Munasinghe for helping design the research study and collecting the data. We are grateful to the participants for sharing their thoughts and experiences with us. Thanks are due to the members of the Human-Centered Computing (HCC) seminar at the University of Utah for comments and suggestions on draft versions of the manuscript. We acknowledge anonymous reviewers for providing valuable feedback that helped us improve the manuscript. The research was supported with funding from the AT&T endowment to the Media and Information department at Michigan State University, where the second author was based when the data was collected.

Appendix A. Screening questionnaire

[NOTE: We sent the following screening questionnaire to those interested in participating in the study. Potential participants could choose not to answer any questions they did not wish to answer. We used the answers to the screening questionnaire to determine eligibility for the study and select participants who formed a sample with diverse practices related to providing made-up email addresses.]

Please answer the following questions. We will use your answers to determine your eligibility for a research study about managing unwanted email. Answering these questions is voluntary. You do not have to answer any questions you do not wish to answer. However, if you do not answer certain questions, we may not be able to determine whether

you are eligible to participate in the study. If you are eligible to participate, we will contact you to schedule an interview at your convenience, either in person, over the phone, or via video conference.

- Are you at least 18 years old?
  - Yes
  - No
- What is your gender?
  - Man
  - Woman
  - Prefer not to disclose
  - Other [Text Box]
- Are you an undergraduate student?
  - Yes
  - No
- How many email addresses do you have?
  - 0
  - 1
  - 2
  - 3+
- How often do you check your email?
  - Almost constantly
  - Several times per day
  - Once per day
  - A few times per week
  - Fewer than once per week
- Can you remember the last time you created a new email address?
  - Yes
  - No
- Have you set up custom rules or filters to organize your Inbox?
  - Yes
  - No
- What percentage of the email messages you receive would fall into each of the following categories? (*The total must sum to 100.*):
  - Personal email messages: [Text box]
  - Work email messages: [Text box]
  - Advertisements & promotional email messages: [Text box]
  - Spam email messages: [Text box]
  - Total: [Auto-calculated]
- Which of the following statements describe you? (*Check all that apply.*)
  - ☐ I have made up an email address on the spot to avoid giving out my email address.
  - ☐ I have given out a slightly different version of my email address.
  - ☐ I have given out a random email address instead of mine.
  - ☐ I have entered the shortest possible combination of characters that could pass as a valid email address when entering my email address online.
  - ☐ I have refused to provide my email address when someone asked for it.
  - ☐ None of the above.
- During the interview, we will ask you to explain how you organize and manage your Inbox. Are you willing to show us your Inbox to help guide that conversation?
  - Yes, and I have a laptop I can bring to an in-person interview.
  - Yes, but I will need to log in on a computer you provide.
  - No.

Appendix B. Semi-structured interview protocol

The semi-structured interview protocol was organized into four broad themes:

B.1. General email use

I would like to start by learning a bit about how you typically use email.

- How often do you check your email?
- How many different email addresses do you have?
- For each of those email addresses, what is its primary use (e.g., interpersonal communication, work, school, receiving promotional offers, etc.)?
- For any email addresses other than your main personal or work email addresses, why did you create that account?
- Which of those email addresses do you use the most?

  For this email address:
  - What kinds of email messages do you receive at this email address?
    - If the participant mentions promotional offers/advertisements:
      - Are you interested in the promotional offers you receive?
      - Do you use the information contained in these email messages?

        [If yes:] How?
    - If the participant mentions spam/junk:
      - What makes you consider these email messages as spam/junk?

Now, we will move on to the section of the interview where you walk us through how your Inbox is organized. When we invited you to participate in this study, we asked if you would be willing to show us your Inbox. Keeping in mind that we will not record or save any specific or identifying information about the contents of your Inbox, please log in to your email account if you still feel comfortable doing so.

[NOTE: We expected the participant to show us the Inbox for the account associated with the email address the participant used the most. However, the participant was free to choose any email account.]

- As you log in to your account or load the page, what is your first reaction to the state of your Inbox?
- Please click through a couple of built-in tabs and folders your email provider uses to categorize your email messages automatically.

  For each specific folder:
  - Please choose one of the email messages in this folder.

    [NOTE: This question block was repeated twice to cover two email messages.]
    - Please describe the message and give me some background on it.
    - Why do you think your email provider classified this email message as [label of the specific folder]?
  - Other than these types of email messages (e.g., interpersonal, work-related, etc.), do you notice any other patterns in which email messages get classified as [label of the specific folder]?
  - Do you see any email messages in this folder for which it does not make sense to you why your email provider classified them as [label of the specific folder]?
    - Why does it not make sense that this message is classified as [label of the specific folder]?
    - Which folder would you prefer it be put into?
    - How do you feel about it being miscategorized? How does the miscategorization affect you?
    - Would you ever manually move it to your preferred folder or flag it as some other category instead? Why/why not?
- [If the participant has custom folders set up:]
  - Why did you create these custom folders?
  - Do you manually move items to these folders? Why/why not?
  - Would you ever set up rules to filter messages into these folders automatically? How easy or difficult would you imagine that to be?
- [If the participant does not have custom folders set up:]

- Have you ever tried creating custom folders to help organize your email? Why/why not?
- Do you know how to do that?

- How do you handle unwanted email messages?
- Please click on the "Trash" folder.
  - Please choose one of the email messages in this folder.
    [NOTE: This question block was repeated twice to cover two email messages.]
    - Please describe the message and give me some background on it.
    - Why did you choose to discard this email message?
    - [If the message is unread:] I see that this message is still unread. What made you delete it without reading it?
    - [If the message is read:] I see that you previously opened this message:
      - Did you read the message before deleting it? Why/why not?
      - Why did you not delete it without reading, based only on the subject/sender?
  - Are there any other types of email messages you tend to delete?
- Please click on the "Spam/Junk" folder:
  - Please choose one of the email messages in this folder.
    [NOTE: This question block was repeated twice to cover two email messages.]
    - Please describe the message and give me some background on it.
    - Why do you think your email provider classified this message as spam/junk?
    - Do you agree that this message is spam/junk? Why/why not?
  - Are there any email messages you would classify as spam/junk that are not sent to this folder? Why/why not?
  - Do you manually flag things as spam/junk?
    [If yes:] Why? How long does that usually take?

B.2. Experiences of giving out made-up email addresses

In the pre-interview screening questionnaire you completed, we asked about situations where you might have provided made-up email addresses. Based on your answers in the questionnaire, we would like to discuss in depth your experiences of providing made-up email addresses.

B.2.1. Slightly different form of the participant's email address

[If 'I have given out a slightly different version of my email address' was selected in the pre-interview screening questionnaire:]

- You said you have given out a slightly different version of your email address. Could you tell me briefly about the last time you did that?
- Who or what company/service asked for your email address?
- Why did you choose to provide a slightly different version of your email address?
- Was it important that the email address you provided resemble one that might belong to someone with your name? Why or why not?
- Do you remember the changes you made to your email address?
  [If yes:]
  - What is your email address, and what was the different version you created?
  - Why did you choose to change your email address in that particular way?
- Imagine that you were in the same situation again. Knowing how it turned out when you did it in real life, would you still provide a different version of your email address instead of yours?
  [If yes:]
  - Could you please write down the email address you would provide this time?
  - Could you explain the thought process behind constructing that email address?
- Do you have any other examples of giving out an email address slightly different from yours?

[If 'I have given out a slightly different version of my email address' was NOT selected in the pre-interview questionnaire:]

- Have you ever given out a slightly different version of your email address?
  [If no:]
  - Would you ever consider doing that? Why or why not?
  - Could you give me an example of a situation where you might consider doing that?
  - Why would that situation make you consider doing it?

B.2.2. Random email address

[If 'I have given out a random email address instead of mine' was selected in the pre-interview screening questionnaire:]

- You said you have given out a random email address instead of yours. Could you tell me briefly about the last time you did that?
- Who or what company/service asked for your email address?
- Why did you choose to provide a random email address instead of yours?
- Do you remember the email address you provided or how you decided on the random email address?
  [If yes:] What was it? Could you please write it down?
- Imagine that you were in the same situation again. Knowing how it turned out when you did it in real life, would you still provide a random email address instead of yours?
  [If yes:]
  - Could you please write down the email address you would provide this time?
  - Could you explain the thought process behind constructing that email address?
- Do you have any other examples of giving out a random email address?

[If 'I have given out a random email address instead of mine' was NOT selected in the pre-interview screening questionnaire:]

- Have you ever given out a random email address instead of yours?
  [If no:]
  - Would you ever consider doing that? Why or why not?
  - Could you give me an example of a situation where you might consider doing that?
  - Why would that situation make you consider doing it?

B.2.3. Shortest acceptable email address

[If 'I have entered the shortest possible combination of characters that could pass as a valid email address when entering my email address online' was selected in the pre-interview screening questionnaire:]

- You said you have entered the shortest combination of characters that could pass as a valid email address instead of giving out your email address. Could you tell me briefly about the last time you did that?
- Who or what company/service asked for your email address?
- Why did you choose to give out this email address instead of yours?
- Why did you choose to give out the shortest acceptable email address instead of a more realistic one?
- Do you remember the short email address you provided?
  [If yes:] What was it? Could you please write it down?
- Imagine that you were in the same situation again. Knowing how it turned out when you did it in real life, would you still provide the shortest acceptable email address?
  [If yes:]
  - Could you please write down the email address you would provide this time?
  - Could you explain the thought process behind constructing that email address?
- Do you have other examples of giving out the shortest acceptable email address?

[If 'I have entered the shortest possible combination of characters that could pass as a valid email address when entering my email address online' was NOT selected in the pre-interview screening questionnaire:]

- When filling out an online form, have you ever provided the shortest combination of characters that could pass as a valid email address instead of giving out your email address?
  [If no:]
  - Would you ever consider doing that? Why or why not?
  - Could you give me an example of a situation where you might consider doing that?
  - Why would that situation make you consider doing it?

B.2.4. Other email address

- Do you have any other examples of giving out an email address you made up on the spot instead of giving out your email address?
- Could you tell me briefly about the last time you did that?
- Who or what company/service asked for your email address?
- Why did you choose to make up an email address on the spot instead of giving out your email address?
- Do you remember how you decided what email address to make up? [If yes:] What was it? Could you please write it down?
- Do you remember if you needed to receive email messages from that sender?
- Imagine that you were in that same situation again. Knowing how it turned out when you did it in real life, would you still provide a made-up email address instead of yours?
  [If yes:]
  - Could you please write down the email address you would provide this time?
  - Could you explain the thought process behind constructing that email address?
- Do you have any other examples of giving out an email address you made up on the spot?

B.2.5. Declining to provide an email address

[If 'I have refused to provide my email address when someone asked for it.' was selected in the pre-interview screening questionnaire:]

- You said you have refused to provide your email address when someone asked for it. Could you tell me briefly about the last time you did that?
- Who or what company/service asked for your email address?
- Why did you not want to provide your email address?
- [If the party who asked for the email address was a person:] How did you feel when refusing to provide an email address?
- If you did not want to give your email address, why did you not make one up?

B.3. Scenarios of being asked for an email address

Now, we will role-play some situations in which a person or a website asks for your email address.

B.3.1. Shopping at a store

Imagine that you are out shopping at a store. When you are checking out at the cash register, the cashier asks for your email address so the store can send you an electronic receipt.

- Have you ever been in a situation like this?
  [If yes:]
  - Could you tell me a little about that?
  - How did you feel about giving out your email address then?
- Imagine you are in that situation again right now, which email address would you give out?
- [If the participant would give out the participant's email address:] Would you ever make up an email address to give out in a situation like this? If yes/maybe, why? If not, why not?
- [If the participant would not choose to give out a made-up email address:] You know that you can ask for a paper receipt at this store, and you do not want to receive any advertisements, promotions, or coupons the store might send because you are not interested in this store. Which email address would you give to the cashier in this case?
- [If the participant would provide/consider providing a made-up email address:]
  - Could you please write down the email address you would provide to the cashier?
  - How did you decide what the made-up email address should be?
  - What do you expect to happen after giving out that made-up email address?

B.3.2. Buying a car at a car dealership

Imagine that you are considering buying a new car and have been going to various dealerships to view and test drive various models. After showing you the available vehicles, the salesperson asks for your email address.

- Have you ever been in a situation like this?
  [If yes:]
  - Could you tell me a little about that?
  - How did you feel about giving out your email address then?
- Imagine you are in that situation again right now, which email address would you give out?
- [If the participant would give out the participant's email address:] Would you ever make up an email address to give out in a situation like this? If yes/maybe, why? If not, why not?
- [If the participant would not choose to give out a made-up email address:] After looking at all models, you have decided that you are not interested in any. Still, the salesperson keeps asking for your email address. You may end up receiving a flood of advertisements from this dealership if you provide your email address. Since you do not wish to purchase a car from this dealership, which email address would you give to the salesperson in this case?
- [If the participant would provide/consider providing a made-up email address:]
  - Could you please write down the email address you would provide to the salesperson?
  - How did you decide what the made-up email address should be?
  - What do you expect to happen after giving out that made-up email address?

B.3.3. Encountering a paywall on a streaming service

Imagine that you are using a new online streaming service. After streaming a few videos, you encounter a paywall that requires you to create an account on the platform for a paid subscription to the service. You can get a one-month free trial before the platform asks for your credit card information. When creating your account, you are asked to provide your name and email address.

- Have you ever been in a situation like this?
  [If yes:]
  - Could you tell me a little about that?
  - How did you feel about giving out your email address then?
- Imagine you are in that situation again right now, which email address would you give out?
- [If the participant would give out the participant's email address:] Would you ever make up an email address to give out in a situation like this? If yes/maybe, why? If not, why not?
- [If the participant would not choose to give out a made-up email address:] The first time you created your account, you used your email address. You remember that the service did not email you to confirm your account creation. After your free trial expires, you realize you could probably get another free trial using a different email address. Which email address would you use to make a second account for another free trial?

- [If the participant would use the participant's email address:]
  - Why did you use your email address?
  - [If the participant mentions having multiple email addresses:] Which of your email addresses did you use (e.g., primary email account)?
- [If the participant would use/consider using a made-up email address:]
  - Could you please write down the email address you would provide to the service the second time?
  - How did you decide what the made-up email address should be?
  - What do you expect to happen after giving out that made-up email address?

B.4. Wrap-up

We have been discussing giving out an email address that is not yours, but one you made up on the spot. We are trying to think of terms to describe such an email address and would like to know what term would make sense to you.

- In fewer than five words, what would you call an email address you provided that does not belong to you?
- In fewer than five words, how would you describe a person who provides an email address that is not the person's email address?

Data availability

Data will be made available on request.

References

Ackerman, M.S., Cranor, L.F., Reagle, J., 1999. Privacy in e-commerce: examining user scenarios and privacy preferences. In: Proceedings of the 1st ACM Conference on Electronic Commerce. Association for Computing Machinery, New York, NY, USA, pp. 1–8, https://doi.org/10.1145/336992.336995

Akbar, F., Bayraktaroglu, A.E., Buddharaju, P., Da Cunha Silva, D.R., Gao, G., Grover, T., Gutierrez-Osuna, R., Jones, N.C., Mark, G., Pavlidis, I., Storer, K., Wang, Z., Wesley, A., Zaman, S., 2019. Email makes you sweat: examining email interruptions and stress using thermal imaging. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, pp. 1–14, https://doi.org/10.1145/3290605.3300898

Alase, A., 2017. The interpretative phenomenological analysis (IPA): a guide to a good qualitative research approach. Int. J. Educ. Lit. Stud. 5, 9–19. https://doi.org/10.7575/aiac.ijels.v.5n.2p.9

Altman, I., 1975. The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding. Brooks/Cole Publishing Company, Monterey, CA, USA.

Arnold, M., Goldschmitt, M., Rigotti, T., 2023. Dealing with information overload: a comprehensive review. Front. Psychol. 14, https://doi.org/10.3389/fpsyg.2023.1122200

Bentley, F., Daskalova, N., Andalibi, N., 2017. "If a person is emailing you, it just doesn't make sense": exploring changing consumer behaviors in email. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, pp. 85–95, https://doi.org/10.1145/3025453.3025613

Bhagyavati, Rogers, N., Yang, M., 2004. Email filters can adversely affect free and open flow of communication. In: Proceedings of the Winter International Symposium on Information and Communication Technologies. Trinity College Dublin, pp. 1–6.

Biczók, G., Chia, P.H., 2013. Interdependent privacy: let me share your data. In: Sadeghi, A.R. (Ed.), Financial Cryptography and Data Security. Springer Berlin Heidelberg, Belin, Heidelberg, pp. 338–353, https://doi.org/10.1007/978-3-642-39884-1_29

Boerman, S.C., Kruikemeier, S., Bol, N., 2021. When is personalized advertising crossing personal boundaries? How type of information, data sharing, and personalized pricing influence consumer perceptions of personalized advertising. Comput. Hum. Behav. Rep. 4, https://doi.org/10.1016/j.chbr.2021.100144

Captain, S., 2024. Should you make up personal information when signing up with websites? Wall St. J. https://www.wsj.com/tech/cybersecurity/website-privacy-security-safety-signups-dc570698 (Accessed: 2024-Dec-11).

Cases, A.S., Fournier, C., Dubois, P.L., Tanner, J.F., 2010. Web site spill over to email campaigns: the role of privacy, trust and shoppers' attitudes. J. Bus. Res. 63, 993–999. https://doi.org/10.1016/j.jbusres.2009.02.028. Advances in Internet Consumer Behavior & Marketing Strategy.

Chen, B.X., 2023. Everyone wants your email address. Think twice before sharing it. The New York Times. https://www.nytimes.com/2023/01/25/technology/personaltech/email-address-digital-tracking.html (Accessed 2024-Aug-19).

Daskalova, N., Bentley, F.R., Andalibi, N., 2017. It's all about coupons: exploring coupon use behaviors in email. In: Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, pp. 1152–1160. https://doi.org/10.1145/3027063.3053339.

Dev, J., Rader, E., Patil, S., 2020. Why Johnny can't unsubscribe: barriers to stopping unwanted email. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, pp. 1–12, https://doi.org/10.1145/3313831.3376165

Ducheneaut, N., Bellotti, V., 2001. E-mail as habitat: an exploration of embedded personal information management. Interactions 8, 30–38. https://doi.org/10.1145/382899.383305

Englehardt, S., Han, J., Narayanan, A., 2018. I never signed up for this! Privacy implications of email tracking. Proc. Priv. Enhancing Technol. 2018, 109–126. https://doi.org/10.1515/popets-2018-0006

Fisher, R.J., 1993. Social desirability bias and the validity of indirect questioning. J. Consum. Res. 20, 303–315. https://doi.org/10.1086/209351

Grevet, C., Choi, D., Kumar, D., Gilbert, E., 2014. Overload is overloaded: email in the age of Gmail. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, pp. 793–802, https://doi.org/10.1145/2556288.2557013

Gruss, D., Schwarz, M., Wübbeling, M., Guggi, S., Malderle, T., More, S., Lipp, M., 2018. Use-after-Freemail: generalizing the use-after-free problem and applying it to email services. In: Proceedings of the 2018 Asia Conference on Computer and Communications Security. Association for Computing Machinery, New York, NY, USA, pp. 297–311, https://doi.org/10.1145/3196494.3196514

Guest, G., Bunce, A., Johnson, L., 2006. How many interviews are enough?: An experiment with data saturation and variability. Field Methods 18, 59–82. https://doi.org/10.1177/1525822X05279903

Hancock, J., Birnholtz, J., Bazarova, N., Guillory, J., Perlin, J., Amos, B., 2009. Butler lies: awareness, deception and design. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, pp. 517–526, https://doi.org/10.1145/1518701.1518782

Hartemo, M., 2021. Conversions on the rise – modernizing e-mail marketing practices by utilizing volunteered data. J. Res. Interact. Mark. 16, 585–600. https://doi.org/10.1108/JRIM-03-2021-0090

Hsiao, J.C.Y., Bentley, F., 2021. Exploring email-prompted information needs. Proc. ACM Hum.-Comput. Interact. 5, https://doi.org/10.1145/3479861

John, T., Wullf, S., 2024. Shorter texts, less scrolling, more visual support for younger learners: low-threshold GDPR conform registration form with double opt-in for the learning management system Moodle. In: Proceedings of the 16th International Conference on Computer Supported Education. Institute for Systems and Technologies of Information, Control and Communication (INSTICC), Science and Technology Publications, Lda, Setúbal, Portugal, pp. 396–403, https://doi.org/10.5220/0012635700003693

Johnson, D.I., Roloff, M.E., Riffee, M.A., 2004. Politeness theory and refusals of requests: face threat as a function of expressed obstacles. Commun. Stud. 55, 227–238. https://doi.org/10.1080/10510970409388616

Jones, S.L., Kelly, R., 2018. Dealing with information overload in multifaceted personal informatics systems. Hum.-Comput. Interact. 33, 1–48. https://doi.org/10.1080/07370024.2017.1302334

Joung, Y.J., Yang, C.J., 2009. Email licensing. J. Netw. Comput. Appl. 32, 538–549. https://doi.org/10.1016/j.jnca.2008.11.003

Ju, J., Cho, D., Lee, J.K., Ahn, J.H., 2021. Can it clean up your inbox? Evidence from South Korean anti-spam legislation. Prod. Oper. Manag. 30, 2636–2652. https://doi.org/10.1111/poms.13398

Kang, R., Brown, S., Kiesler, S., 2013. Why do people seek anonymity on the internet? Informing policy and design. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, pp. 2657–2666, https://doi.org/10.1145/2470654.2481368

Kern, M., Ohly, S., Ďuranová, L., Friedrichs, J., 2024. Drowning in emails: investigating email classes and work stressors as antecedents of high email load and implications for well-being. Front. Psychol. 15, https://doi.org/10.3389/fpsyg.2024.1439070

Kubicek, K., Merane, J., Bouhoula, A., Basin, D., 2024. Automating website registration for studying GDPR compliance. In: Proceedings of the ACM Web Conference 2024. Association for Computing Machinery, New York, NY, USA, pp. 1295–1306, https://doi.org/10.1145/3589334.3645709

Letmathe, P., Noll, E., 2024. Analysis of email management strategies and their effects on email management performance. Omega 124, https://doi.org/10.1016/j.omega.2023.103002

Marshall, B., Cardon, P., Poddar, A., Fontenot, R., 2013. Does sample size matter in qualitative research? A review of qualitative interviews in IS research. J. Comput. Inf. Syst. 54, 11–22. https://doi.org/10.1080/08874417.2013.11645667

Maseeh, H.I., Jebarajakirthy, C., Pentecost, R., Arli, D., Weaven, S., Ashaduzzaman, M., 2021. Privacy concerns in e-commerce: a multilevel meta-analysis. Psychol. Mark. 38, 1779–1798. https://doi.org/10.1002/mar.21493

McDonald, A., Sugatan, C., Guberek, T., Schaub, F., 2021. The annoying, the disturbing, and the weird: challenges with phone numbers as identifiers and phone number recycling. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, pp. 1–14, https://doi.org/10.1145/3411764.3445085

Micheaux, A.L., 2011. Managing e-mail advertising frequency from the consumer perspective. J. Advert. 40, 45–66. https://doi.org/10.2753/JOA0091-3367400404

Nissenbaum, H., 2004. Privacy as contextual integrity. Wash. Law Rev. 79, 119–157. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10.

Palen, L., Dourish, P., 2003. Unpacking "privacy" for a networked world. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, pp. 129–136, https://doi.org/10.1145/642611.642635

Petronio, S., 2002. Boundaries of Privacy: Dialectics of Disclosure, SUNY Series in Communication Studies. State University of New York Press, Albany, NY, USA.

Popescu, M., Baruh, L., 2013. Captive but mobile: privacy concerns and remedies for the mobile environment. Inf. Soc. 29, 272–286. https://doi.org/10.1080/01972243.2013.825358

Rader, E., Munasinghe, A., 2019. "Wait, do I know this person?": Understanding misdirected email. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, pp. 1–13, https://doi.org/10.1145/3290605.3300520

Rauti, S., 2019. An inquiry into localized email SPAM. In: Proceedings of the 20th International Conference on Computer Systems and Technologies. Association for Computing Machinery, New York, NY, USA, pp. 42–48, https://doi.org/10.1145/3345252.3345298

Saldaña, J., 2021. The Coding Manual for Qualitative Researchers, Fourth ed. SAGE Publications Ltd., Thousand Oaks, CA, USA.

Senol, A., Acar, G., Humbert, M., Borgesius, F.Z., 2022. Leaky forms: a study of email and password exfiltration before form submission. In: 31st USENIX Security Symposium. USENIX Association, Boston, MA, pp. 1813–1830, https://www.usenix.org/conference/usenixsecurity22/presentation/senol.

Serewicz, M.C.M., Petronio, S., 2007. Communication privacy management theory. In: Whaley, B.B., Samter, W. (Eds.), Explaining Communication: Contemporary Theories and Exemplars. Lawrence Erlbaum Associates Publishers, Mahwah, NJ, USA, pp. 285–304.

Sergeeva, A., Rohles, B., Distler, V., Koenig, V., 2023. "We need a big revolution in email advertising": users' perception of persuasion in permission-based advertising emails. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, https://doi.org/10.1145/3544548.3581163

Shukla, S., Misra, M., Varshney, G., 2024. Email bombing attack detection and mitigation using machine learning. Int. J. Inf. Secur. 23, 2939–2949. https://doi.org/10.1007/s10207-024-00871-7

Sudhodanan, A., Paverd, A., 2022. Pre-hijacked accounts: an empirical study of security failures in user account creation on the web. In: 31st USENIX Security Symposium. USENIX Association, Boston, MA, pp. 1795–1812, https://www.usenix.org/conference/usenixsecurity22/presentation/sudhodanan.

Tarafdar, M., Wenninger, H., Stich, J.F., 2023. Email overload: investigating technology-fit antecedents and job-related outcome. SIGMIS Database 54, 77–96. https://doi.org/10.1145/3595863.3595869

The Radicati Group, Inc., 2023. Email Statistics Report, 2023–2027. https://www.radicati.com/wp/wp-content/uploads/2023/04/Email-Statistics-Report-2023-2027-Executive-Summary.pdf (Accessed 2024-Sep-9).

Usman, W., Hu, J., Wilson, M., Zappala, D., 2023. Distrust of big tech and a desire for privacy: understanding the motivations of people who have voluntarily adopted secure email. In: Nineteenth Symposium on Usable Privacy and Security. USENIX Association, Anaheim, CA, pp. 473–490, https://www.usenix.org/conference/soups2023/presentation/usman.

Whittaker, S., Sidner, C., 1996. Email overload: exploring personal information management of email. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, pp. 276–283, https://doi.org/10.1145/238386.238530

Wood, K.E., Krasowski, M.D., 2020. Academic e-mail overload and the burden of "academic spam". Acad. Pathol. 7, https://doi.org/10.1177/2374289519898858