Abstract. Social network users may wish to preserve their anonymity online by masking their identity and not using language associated with any particular demographics or personality. However, they have no control over the language in incoming communications. We show that linguistic cues in public comments directed at a user are sufficient for an accurate inference of that user’s gender, age, religion, diet, and even personality traits. Moreover, we show that directed communication is even more predictive of a user’s profile than the user’s own language. We then conduct a nuanced analysis of what types of social relationships are most predictive of users’ attributes, and propose new strategies on how individuals can modulate their online social relationships and incoming communications to preserve their anonymity.

1 Introduction

Communication is the crux of online social platforms and the messages people write can reveal substantial information about their identity, such as their demographic attributes, personality, location, native language, or socioeconomic status. Knowledge of a person’s identity benefits many downstream applications including commercial ones, which has led to a significant effort to develop methods that infer an author’s latent attributes automatically from their writings. Most profiling and demographic inference methods focus on the text an individual writes. However, individuals also communicate directly with others, raising the question of how much incoming messages reveal about a recipient. Further, such directed speech also raises an important privacy concern: although people can opt to self-censor information to reveal less of their identity through the statements they make [63, 2, 62, 85], a person does not control what their friends say to them, potentially exposing much about their identity. Such directed speech can be highly revealing of the individual’s identity and social relationships, as shown in Figure 1. Here, we measure to what degree incoming messages sent to an individual reveal their personal attributes and whether privacy-seeking individuals can obfuscate their own information when they cannot control the content they receive.

![Fig. 1. A real demographically-revealing directed message that conveys age, gender, marital status, and familial relations of the recipients.](image-url)
Prior work on demographic inference has largely focused on analyzing either the individual directly through the text they produce [20] or information from their social network, where friends are assumed to have similar attributes [1, 3]. Here, we consider a third source of information from directed communications to an individual. We hypothesize that directed communication affords multiple channels for revealing personal information, as it has been shown that peers construct a shared identity through language choice [17], that particular expressions are said more to particular social categories, e.g., biased language [33, 25], and that language expresses an asymmetric social relationship linked with social differences, e.g., condescension [92]. Our work offers an important complementary approach to profiling and demographic inference that is applicable even when individuals reduce the amount of personally-identifying statements they make on social media [82, 85] or even employ recent techniques to adversarially prevent their identity from being inferred [77, 114, 15, 112, 88].

Our work provides three main contributions:

- We establish that language in incoming communications is a highly-accurate source of demographic and personal information about an individual. To this end, we develop classifiers for five diverse demographic attributes: age, gender, religion, diet, and personality (§3). Our classifiers—trained on directed communications—learn to discriminate linguistic cues that are closely aligned with personal attributes of the individual to whom these messages are directed. These cues also have close correspondence with prior studies on profiling and demographic inference analyzing linguistic traits characteristic to the social group of the recipient.

- We establish, for the first time, a statistical relationship between (i) the efficacy of incoming communications in user profiling and demographic inference, and (ii) the strength of social ties of interlocutors (§4). We show that incoming communications from an individual’s strong ties are more revealing of the individual’s identity, but that this relationship only holds for publicly-visible aspects of the identity.

- We propose novel adversarial strategies for individuals to use for preserving their privacy (§5). We demonstrate that effective adversarial behavior is possible by strategic recruitment of new peers.

More broadly, our work captures the dual use of Natural Language Processing (NLP) techniques [50] by providing new demographic inference techniques that enable NLP for Social Good applications like mental health assessment [9], while also providing adversarial solutions for individuals who want to participate in social media but need to maximize anonymity for safety reasons [39].

## 2 Language and Identity

Individuals frequently reveal aspects of their social identity through their language choice and style. These choices help individuals associate themselves with a particular identity [37, 17] and in conversation, language choice helps establish a social common ground and implicitly denotes mutual membership in a common social category [55, 34]. Following, we outline some such demographic aspects and how they manifest in speech and social interactions.
2.1 Linguistic Signals of Personal Identity

Individuals make linguistic choices in order to signal their membership in social categories. These categories range from observable demographic attributes like age and gender to those associated with choice like diet and political affiliation. Here, we study five possible categories: gender, age, religion, diet, and extroversion. These categories capture a broad spectrum of possible attributes that affect language choice and include extrinsic, publicly-visible categories (age and gender) and intrinsic, private categories that are not necessarily publicly known by peers (diet, religion, extroversion). These attributes also reflect different computational tasks by including two binary variables (gender and extroversion\(^1\)), two categorical variables (diet, religion) and a continuous-valued variable (age).

**Gender** Gender is known to be one of the most important social categories driving language choice and its study has a long tradition within sociolinguistics [104, 105, 52, 24, 37, 56, 25]. More recent work has begun to examine how gender is expressed in platforms such as Twitter, where the lack of prosodic and non-verbal cues gives rise to other forms of linguistic variation; these purely textual signals have enabled large-scale studies of gender signaling [87, 18, 78, 94, 10, 23, 41, 6, 111, 19, 43, inter alia]. These studies have found a broad range of style and content differences. For example, women are more likely to use pronouns, emotion words (like sad, love, and glad), interjections (ah, hmmm, ugh), emoticons, and abbreviations associated with online discourse (lol, omg), while men tend to use higher frequency standard dictionary words, proper names (e.g., the names of sports teams), numbers, technology words, and links.

**Age** Individuals make language choices that signal their age, which may be intended to convey the speaker’s maturity or express the stage in life [35]. As with gender, textual communication on social media has allowed building computational models for predicting age from language usage, including Twitter [87, 72, 73], blogs [90, 47], Facebook [93], and Netlog, a Dutch social network platform akin to Facebook [78]. The models show clear differences in linguistic choices, with younger individuals performing more stylistic variation like elongation and capitalization [47, 7], grammatical differences in sentence length and construction [49], and content choices to include more self-references, slang, and acronyms [90, 73, 87]. However, for older individuals these differences are less pronounced [74], which obstructs age inference solely from text.

**Diet** Individuals adopt self-imposed dietary restrictions for a variety of medical, religious, or ethical considerations. The impact of this choice may be expressed in the topics they discuss. Prior work has primarily focused on identifying vegetarians [8, 38], suggesting such individual are identifiable from topical features.

**Religion** Religious affiliation provides a social construct that individuals may identify with, akin to race or ethnicity [5, 113]. Affiliations frequently provide metaphors and terminology that work their way into the regular lexicon, which automated methods have leveraged for classifying individuals in social media [75, 21].

**Extroversion** Extroversion is a strong predictor of social engagement with one’s peers and increased social status [4], though the degree of extroversion or introversion has

---

\(^1\) We note that both gender and extroversion may also be considered along a spectrum [37, 36]. We opt to study these as binary variables here due to lack of continuous-valued gender and extroversion ratings for social media users.
not been shown to affect the amount of self-disclosure [95]. Automated methods for personality detection have shown that extroverted individuals tend to use more terms describing social activities and concepts and colloquial language, whereas introverts refer to more solitary activities [30, 45, 86, 96, 53]

2.2 Social Identity in Communication

While an individual’s own speech is predictive of their identity, the communication they receive is also potentially predictive due to the social processes that drive language selection. Following the principle of homophily, individuals tend to have social relationships with others similar to themselves in interests and demographics [66]; the communication within these relationships often focuses on the common ground [91], which can be used to identify their shared demographics. The process of revealing demographically-identifiable information is further supported by the tendency of individuals to reciprocate in self-disclosure in conversation, which provides more evidence of shared identity [29].

2.3 Online Identity and Privacy Protection

Public communication in social media can reveal significant information about a person, which has led some individuals to change their communication strategies to preserve privacy [102]. Individuals modulate these strategies relative to their closeness with the peer and are less likely to self-censor when talking with close friends [103]. In addition, anonymization strategies vary both demographically, e.g., females are more likely to use misinformation to preserve their privacy [77, 114], and culturally, e.g., cultures with collectivist tendencies tend to censor less [89, 109]. Despite these privacy efforts, an individual’s identity may still be revealed by others’ communication about or to them, e.g., parents compromising their children’s privacy online by revealing their age and location [68], or friends revealing a person’s religion or relationship status [108]. Our work extends this line of research by examining what can be inferred about a person from both explicit and implicit signals in the communications they receive.

3 Profiling via Incoming Communications

Given that a person’s identity is expressed through language, we first examine to what degree incoming communications received by an individual are predictive of that user’s personal attributes discussed in §2.1.

3.1 Data

Individuals for each demographic attribute were collected using targeted queries of the Twitter platform. For gender, we use fixed patterns on user profiles to find individuals who explicitly self-identify with a gender, e.g., “Writer in NY; she/her” or who identify with gendered social roles, e.g., “father to two girls.” Age is identified using fixed patterns with aggressive filtering to remove noise. Diet was collected in a similar manner
<table>
<thead>
<tr>
<th>Attribute</th>
<th># of Tweets</th>
<th>Majority Class</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>59800</td>
<td>Male</td>
<td>52.5</td>
</tr>
<tr>
<td>Religion</td>
<td>19940</td>
<td>Christian</td>
<td>65.8</td>
</tr>
<tr>
<td>Extroversion</td>
<td>24576</td>
<td>Introvert</td>
<td>63.0</td>
</tr>
<tr>
<td>Diet</td>
<td>9001</td>
<td>Unrestricted</td>
<td>41.0</td>
</tr>
<tr>
<td>Age</td>
<td>38134</td>
<td>21.3 (mean)</td>
<td>5.7 (s.d.)</td>
</tr>
</tbody>
</table>

Table 1. Dataset sizes for each demographic attribute and frequencies of the majority classes.

as in El-Arini et al. [38] by identifying individuals who report themselves as vegetarian, vegan, or paleo; we sample an equal number of individuals not reporting these diets and treat them as being examples of the unrestricted diet class. We follow Chen et al. [21] and identify individuals’ religious affiliations by searching for a fixed set of terms in the user profile for the following affiliations: agnostic, atheist, Buddhist, Christian, Hindu, Jewish, Muslim. For personality, we adopt the approach of Plank and Hovy [83] for gathering Myers-Briggs personality type indicators and its Introversion/Extroversion labels, which have been shown to strongly load on the Extroversion dimension of the more-commonly used Big Five personality assessment [51, 65].

Targeted queries were used to find all individuals with matching profiles or tweets during March 2016, except for Extroversion which was queried from January 2010 to December 2016 due to its relative sparsity. Tweets for identified individuals were then collected from a 10% random sample of Twitter from 2014 to 2016. The CLD2 language detector [64] was used to retain only English-speaking individuals. Finally, only those users with at least 100 tweets directed to them are included in the dataset. Table 1 summarizes the resulting dataset.

3.2 Personal Attribute Classifiers

Features An individual’s associated text is represented using content and stylistic features drawn from prior work. The broad themes are represented using a 100-topic LDA model [12], capturing both the average topic distribution for a message and the maximum probability a topic ever receives. A lexicon learned for each attribute was constructed by ranking all unigrams and bigrams using the weighted log-odds-ratio with an informative Dirichlet prior [70]. To construct binary classes for computing the log-odds of multiclass attributes, we chose one attribute relative to all the other attributes in the class; for age, lexicons were created by discretizing age into decade ranges (e.g., age 20-29) and computing the log-odds for that decade relative to the others. Content was additionally categorized using the Linguistic Inquiry and Word Count (LIWC) dictionary [106] and the average GloVe vector computed from all words received by an individual [81].

Stylistic features include pronoun usage, disfluencies, laughing expressions, question frequencies, average word length, usage of capital letters, word lengthening, and punctuation [80, 7, 47, 87, 90, 73, 23]. We also include emoji usage, which are language-independent signals that carry social status [107, 60], a general lexicon for sentiment

---

2 We note that other diets are possible, such as kosher or halal; however, these are closely related to religion, which we also study, so we intentionally exclude them.

3 Additional queries were formed for Sikhism and Jainism which did not return sufficient numbers of English speaking individuals to be included.
and second sentiment lexicon focused on the extremes [61], which was shown to be effective for distinguishing different personality types, and lexicons with concreteness and abstractness ratings [16]. Ultimately, 2,625 features are used.

**Models** Categorical attributes are predicted using random forest classifiers [14], an ensemble of decision tree classifiers learned from many independent subsamples of the training data; age is predicted using a random forest regressor. Random forest ensembles are particularly suitable for imbalanced multilabel setups such as ours and have been shown to be robust to overfitting when using many features [40]. Separate models were trained for each attribute. Models are evaluated using ten-fold cross-validation using Macro- and Micro-F1 for categorical attributes (see Appendix A) and the numeric age predictions are evaluated using Mean Squared Error and Pearson’s $r$

**Baselines** We evaluate against two systems that use the same textual features but calculate them based on (1) the individual’s outgoing language, rather than directed to them and (2) the language of the individual’s peers, not necessarily directed towards the individual. For both baselines, we use the same ground truth individuals and recalculate the log-odds lexicons and topic models on their respective text. These models capture the information available through self-disclosure and from homophily, respectively, and are broadly representative of many related works for each attribute. To ensure a fair comparison with the incoming-text model, we evaluate each model on individuals that have 100 tweets authored by themselves or their peers, respectively. Finally, we include a baseline system that predicts the most frequent class or the mean numeric value.

### 3.3 Results

The language of incoming communications was highly predictive of recipients’ demographic attributes, matching or surpassing the performance of the recipient’s own speech and that of their peers for all attributes but age, as shown in Figure 2. The performance of the directed speech classifier for each attribute is close to current state-of-the-art methods, e.g., [22], which typically also include features from the social network, biography, and other sources. Performance across attributes varied widely; the highest improvement relative to other forms of communication was seen for gender. This is expected, as individuals may be referred to by gendered categories in discourse. For example, the following tweets provide a clear lexical signal: “@User bro u don’t even know my squad lol tf” and “@User Sounds great! Are you ladies going to #DisruptHRTO?”. Our results build upon multiple findings from sociolinguistics that directed speech can reveal significant information by individuals accommodating linguistic style of their peers [76, 26], that individuals sharing the same attribute are more likely to use a common vernacular that indicate in-group status [67], and that dialog is conducive to self-disclosure [29].

Examining the feature importance for each attribute’s classifier, we find that features based on the log-odds bootstrapped lexicons, topical differences, and the average word vector of received messages account for the majority of the most discriminative features. This trend matches the prior observation that machine-learned topic features are highly effective at distinguishing between demographics [79]. Examining the log-odds bootstrapped lexicons, the words most biased towards particular demographic attributes mirrored categories seen in self-speech, such as speech towards women including more
emotion words and towards younger ages including more non-standard spellings and abbreviations. In addition, the log-odds lexicons captured topical preferences by gender, such as school terms for younger demographics, foods associated with the different diets, and religion-affiliated language. Table 2 shows examples of words from received communication that are most-biased towards particular demographic attributes. When an attribute’s log-odds lexicon was highly weighted by the classifier, we found significant overlap with its most-biased words and the linguistic cues expected in self-speech when an individual signals their own social category. This overlap suggests that these demographically-biased words represent a common ground for two individuals with shared identity [37, 17] and the relative importance of such words for classification indicates they are key features as individuals signal their identity in dialog.

As a follow-up experiment, we calculated the learning curve for each classifier to test how many peers are needed to obtain high performance. Curves were estimated by repeatedly sampling up to 100 peers for each user and estimating performance. Learning curves, shown in Figure 3, reveal that most performance gains are seen with just a few peers and diminishing gains after 20 friends. These trends suggest that attributes can be reliably inferred from limited peer evidence, which substantially reduces the data collection effort needed to per user.
Table 2. Examples of the most salient words used in directed speech (incoming communications) towards people with a particular attribute, learned from log-odds with a Dirichlet prior [70]. The right column lists what linguistic cues are expected to be observed in individual’s texts (outgoing communications), based on prior work, summarized in §2.1. Strong linguistic and topical correspondence between outgoing and incoming communications enables training effective profiling classifiers without any text produced by a person, as proposed in §3.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Most Salient Words in Incoming Communications</th>
<th>Characteristic Cues Used By People to Signal Their Own Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>Male: team, mate, coach, players, nfl, his, teams, games, player, football, man, matt, play she, love, she, beautiful, gift, entered, girl happy, thank, lovely, mom, christmas, cute</td>
<td>Frequent words, names, sports teams.</td>
</tr>
<tr>
<td></td>
<td>Female: her, love, she, beautiful, gift, entered, girl happy, thank, lovely, mom, christmas, cute</td>
<td>Pronouns, emotion words, interjections.</td>
</tr>
<tr>
<td>Religion</td>
<td>Christian: pjnet, catholic, obama, deplorable, trump, christian, amen, bless, church, america, prolife atheist, atheism, atheists, evolution, shit, fuck, science, evidence, fucking</td>
<td>Words from a particular religious affiliation.</td>
</tr>
<tr>
<td></td>
<td>Atheist: atheist, atheism, atheists, science, evolution, shit, fuck, sex, evidence, fucking</td>
<td>More words from scientific and political topics.</td>
</tr>
<tr>
<td>Age</td>
<td>10–19: birthday, happy, whooo, via, iloveyou, coolest, hemmings, stepfather, wvu, thanks, gotham trump, obama, great, verified, win, news, deplorable, daily, latest, john, book, read</td>
<td>More stylistic and grammatical variation, self-references, slang, and acronyms.</td>
</tr>
<tr>
<td></td>
<td>30–39: Less linguistic variation, speaker’s maturity.</td>
<td></td>
</tr>
</tbody>
</table>

Fig. 3. Learning curves of how predictive accuracy changes relative to how many peers’ communications are used for prediction. Shaded regions show bootstrapped 95% confidence intervals.

4 Demographic Inference and Tie Strength

Individuals engage with a variety of users on Twitter, from close friends to complete strangers; these different types of relationships can be categorized into strong and weak social ties [48]. Communication is driven in part by the strength of social ties [13]. For example, close friends may be more likely to discuss more intimate and immediate topics (e.g., dinner plans), whereas less-familiar acquaintances may use more formal language and relate to the person less as an individual and more as their social categories (e.g., gender, political affiliation) [100, 84, 57]. This observation motivates our research hypothesis that the message content of close friends reveals more of the recipient’s demographics than the more stereotypical language of socially-distant peers. In this section, we use statistical inference to examine whether the directed speech generated from strong ties is more predictive of the recipient’s identity.
Table 3. Regression models showing the impact of increased tie strength (calculated via proxies discussed in §4.1) on a peer’s predictive accuracy. The categorical variable for Relationship has the reference coding of “No Relationship” for all models. Note that since the Age regression is on Error instead of accuracy, its coefficients’ interpretations are reverse of those of other attributes.

<table>
<thead>
<tr>
<th></th>
<th>Gender</th>
<th>Religion</th>
<th>Diet</th>
<th>Extroversion</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication Frequency</td>
<td>0.032***</td>
<td>−0.049</td>
<td>0.147</td>
<td>0.105</td>
<td>−0.190***</td>
</tr>
<tr>
<td>Relationship: peer-follows</td>
<td>0.264***</td>
<td>0.365</td>
<td>0.303</td>
<td>−0.179</td>
<td>−0.051</td>
</tr>
<tr>
<td>Relationship: ego-follows</td>
<td>0.270***</td>
<td>0.336</td>
<td>−0.235</td>
<td>−0.263</td>
<td>0.085</td>
</tr>
<tr>
<td>Relationship: reciprocal</td>
<td>0.243***</td>
<td>0.556***</td>
<td>0.059</td>
<td>−0.056</td>
<td>−0.535***</td>
</tr>
<tr>
<td>Intercept</td>
<td>0.687***</td>
<td>0.384**</td>
<td>0.510**</td>
<td>1.584***</td>
<td>4.539***</td>
</tr>
</tbody>
</table>

Marginal $R^2$: 1.71e-03, 1.185e-03, 8.123e-04, 2.151e-04, 3.617e-03
Conditional $R^2$: 0.352, 0.937, 0.905, 0.948, 0.836
Observations: 35,962, 10,408, 5,000, 22,819, 12,850

4.1 Tie Strength

Tie strength in social relationships has many dimensions [54]. The four dimensions originally introduced by Granovetter are the amount of time in communication, intimacy, intensity, and reciprocity which characterize the tie [48]. Other dimensions were proposed later, for example social distance [58] and types of social relationships [42]. To capture the tie strength between the speaker and recipient, we use the following proxies, following prior work (also see Appendix C). Communication frequency [48] is operationalized by the number of tweets sent. Explicit social relationships [42] is captured by crawling the friend and followers edges of the individuals on the Twitter network. We consider four types of relationships: (1) the peer follows the individual, (2) the individual follows the peer, (3) both follow each other, (4) no edges.4

4.2 Statistical Inference

We test for the effect of social ties on predictiveness of an individual’s identity by fitting mixed-effect models with random effects for the individual receiving the messages, and fixed-effects models for each proxy for tie strength. Random effects control for variation in the relative predictiveness across individuals. The number of messages sent by peers follows a power-law distribution, so we log-transform the message counts to avoid scaling issues during fitting. Generalized logistic mixed-effect models were fit to the binary dependent variable of whether the peer predicts the correct attribute; linear mixed effect models were fit to the absolute value of the error in age. We measure the amount of variance explained by the mixed-effect models by calculating $R^2$ using the method of Nakagawa and Schielzeth [71]; here, the marginal $R^2$ describes the proportion of variance explained by only the fixed effects (age and social distance); while the conditional $R^2$ measure variance from the fixed and random effects. To avoid data sparsity, we fit the models only with peers who send at least ten messages to a person.

4 Due to Twitter API rate limits, full edge information was gathered only for 1.7M pairs.
4.3 Results

Results are summarized in Table 3. Our models reveal that increased tie strength is significantly associated with a peer’s predictiveness for gender and age. However, no relationship was found for the other three attributes, religion, diet, and extroversion. We speculate that associations were found for gender and age because these attributes are more easily observable: they are frequently signaled by cues such as an individual’s username or profile picture and therefore visible to both strong and weak ties. In contrast, religion, diet, and extroversion can be construed as more internal and not necessarily evident to an individual’s ties, regardless of strength; because these attributes are less known, peers are less likely to modulate their speech on the basis of them.\(^5\)

For gender and age, the majority of proxies for tie strength had a statistically-significant positive association with increased accuracy (gender) or reduced error (age), confirming our hypothesis that stronger ties are more predictive. For age and gender, more communication and having a reciprocal social relationship were consistently positively associated with demographic predictiveness, with additional significant effects seen for gender when individuals have any form of explicit relationship. The Marginal R\(^2\) indicates that tie strength explains only a small part of the variance in predictive accuracy; however, the communications of a single peer alone are unlikely to be highly accurate (cf. the learning curve in Figure 3), which limits establishing a larger fit from the fixed effects.

5 Preserving Anonymity through Adversarial Behavior

Online social platforms can serve a critical need for individuals to engage with others and obtain social, physical, and mental support [11, 28]. When discussing sensitive or controversial topics, individuals often aim to maintain some degree of privacy online [27, 97, 115]. However, in §3 we have shown that even if individuals self-censor their content or employ adversarial strategies to mask their identity [63, 2, 62, 85], the messages they receive can still reveal significant information about them.\(^6\) This loss of privacy is potentially disastrous for individuals discussing politically-sensitive topics, as multiple reports have shown governments to pursue individuals when their identity is revealed [39].

Given the potential loss of privacy from other’s incoming communications, we consider here how a user may still minimize what might be inferred about them. Under the reasonable assumption that an individual has no control over what their existing peers communicate to them (especially weak-tie peers), an alternative option a user has is to adversarially recruit new peers whose messages to them will mask the existing demographic signal. Without the ability to control what is said to them, an individual can no longer rely on adversarial stylometrics to hide their identity [63, 2, 62, 85]. Following, we evaluate the effectiveness of adversarial strategies and then discuss key technical challenges for operationalizing these strategies in real platforms.

5 One possibility for testing this hypothesis in future work is to identify a cohort of individuals who publicly signal these variables in an explicit way (e.g., including religious imagery in their profile picture) and then test for effects of tie strength on their peers’ predictiveness.

6 This risk is valid even if the individual themselves does not engage with others, as platforms such as Twitter allow anyone to directly message another unless banned.
5.1 Adversarial Strategies

We model peer adoption strategies as a friend-of-a-friend recruitment, where individuals have the option of selecting a peer using two parameters: (i) who the peer is and (ii) who the peer is communicating with. For notational simplicity we refer to the individual recruiting a new peer as $u_i$; $u_i$ can select another peer $u_k$ who is communicating with peer $u_j$. Peer communication is simulated as if $u_k$ communicated with $u_i$ instead of $u_j$.

Four adversarial strategies are tested: three folk strategies that an individual might feasibly use on the basis of public information and one strategy that requires knowledge of the classifier.

1. **Random Peer**: the user chooses a random user $u_j$ and then receives communication from a random friend of $u_j$.

2. **Different-Attribute Peer**: the user chooses the peer $u_k$ of a user $u_j$ who has a different demographic attribute than themself; e.g., a woman would choose the peer of a man.

3. **Topic Difference**: the user chooses the peer $u_k$ whose messages to $u_j$ are the most topically dissimilar from the topics seen in the current conversations to $u_i$.

4. **Feature Difference**: This strategy has knowledge of the exact features used by the classifier and the feature vector for the current individual. A new peer is chosen by selecting $u_k$ whose messages to $u_j$ would produce a feature vector that is maximally different from the vector for $u_i$.

When sampling multiple new peers, all strategies sample peers without replacement and the Topic Difference and Feature Difference strategies sample in decreasing order of distance (i.e., the most-different are chosen first).

5.2 Experimental Setup

We repeat the classifier and experimental setup from Section 3 with separate models for each attribute. The effectiveness of adversarial behavior is tested using ten-fold cross-validation where the test fold data alone is used for simulating adversarial behavior; i.e., all new peers selected by an adversarial strategy are chosen from within the test set, which prevents test-train leakage. During testing, we sample an increasing number of new peers for each user and compute the classifier’s accuracy based on the percentage of new peers added relative to the number of prior peers.

5.3 Results

Classifier performance, shown in Figure 4, reveals that adversarial strategies can be effective at reducing performance to chance levels (denoted with a horizontal red line) and even at flipping the perceived attribute of the individual. However, the number of new peers needed to attain these goals varied substantially by strategy and attribute. With knowledge of the classifier’s features, the Feature Difference strategy is able to

---

7 We note that while we measure topical difference using our LDA model for messages, the peers selected by maximizing topical difference would be easily identified as such by the layperson (e.g., a peer discussing completely different topics).
effectively reduce performance to near chance for all but the diet and age attributes; as Figures 4a, 4b, and 4d show, a 25% increase in the number of peers provides effective anonymity for those attributes.

Among the folk strategies, the Different-Attribute Peer and Topic Difference strategies are the most effective, though neither is able to consistently obtain at-chance performance. Both strategies are roughly equivalent for extroversion, diet, and religion, but diverge in their anonymization abilities for gender and age. For gender, Different-Attribute Peer is able to obtain at-chance performance with an 80% increase in new peers, while Topic Difference did not converge to at-chance even after tripling the number of peers a user has. However, for age, Topic Difference provides the highest effectiveness of any strategy. However, overall, folk strategies required far more new peers on average to be effective than the classifier-aware strategy, which is potentially prohibitive for users who already have a large cohort of peers messaging them.

Age and diet are difficult attributes to attain chance-level performance in our dataset. Age obfuscation is made difficult by the age distribution of the platform and textual differences between age groups. Individuals in Twitter are known to skew younger [31] (as also seen in our dataset) and older age groups are known to have fewer textual differences between them [73]; therefore, we speculate that it is difficult to select peers adversarially since there are fewer peers communicating with older individuals whose content is sufficiently dissimilar. We also note that the Different-Attribute Peer strategy could likely be improved by selecting $u_j$ to maximize the difference in age, rather than simply selecting a $u_j$ that has a different age. We speculate that obfuscating diet is difficult due to the nature of the unrestricted-diet class. Vegans, vegetarians, and paleo diet practitioners all have specific dietary restrictions and the topic of these restrictions serves as discriminating features; in contrast, the unrestricted diet is defined by the
absence of these, so new peers with this attribute are much less likely to have a strong lexical signal about their diet that would change the classifier’s prediction.

5.4 Discussion

Our results demonstrate that adversarial strategies can be effective in theory. However, implementing these strategies in practice faces two key challenges. First, our experiment simulates adding new peers as if the content they directed to $u_j$ had been directed to $u_i$. This process assumes that new peers would still communicate with the same type of content as if they had been talking to $u_j$; e.g., if a female adds the peer of a male, the new peer would need to talk to her as if she were that male. In addition, new peers are expected to message with the same frequency, which is potentially unlikely when engaging with strangers.

Second, optimal adversarial behavior should be undetectable by the observing party. However, structural properties of the underlying social network of Twitter can potentially reveal the adversarially-added peers. Specifically, adding new peers would likely add individuals from distant parts of the network making them easier to detect. As a result, an adversarial user must add new peers whose placement in the social network is similar to that of their current peers, which could significantly restrict the available pool of new peers.

We speculate that for the truly adversarial, one option is to create and use sock puppet accounts. These accounts can easily be managed to control their content and to follow existing peers in order to seamlessly integrate into a user’s social network network. A second possibility for mitigating these challenges is changing the self-presentation signals of the account, such as selecting a gender-neutral profile picture and username. These strategies minimize the social signaling of identity in other domains (e.g., job applications, email) and are known to change peers’ behaviors [101, 46].

Finally, our findings have important implications for related work in differential privacy where, when releasing data about users, their privacy is preserved by strategically manipulating (or adding noise to) text that each produces [32]. Our work demonstrates that in order to preserve the anonymity of a person’s demographic attributes, a differential privacy system would need to modify any queries requesting the directed speech to an individual as well—not just the individual’s own speech.

6 Conclusion

We have long known that what you say on social media reveals your identity and may compromise your privacy. Our work shows that even ignoring what you say, just looking at what your friends say to you is generally even more informative, and allows us to guess your gender with 80% accuracy, as well as your age (71.2%), and even your private attributes like your religion (74.4%) and personality traits (67.3%). Moreover, your closer friends reveal more about your publicly-visible identity than more distant ones, but not about your private attributes. Strategic selecting new peers to communicate with can obstruct profiling, but more work needs to be done to safeguard privacy. Code and data used in the experiments are at https://github.com/davidjurgens/profiling-by-directed-speech.
Acknowledgments

We thank the anonymous reviewers, SocInfo organizers, the Stanford Data Science Initiative, and Twitter and Gnip for providing access to part of data used in this study. This work was supported by the National Science Foundation through awards IIS-1159679 and IIS-1526745.

A Classification Metrics

Macro-averaged F1 denotes the average F1 for each class, independent of how many instances were seen for that label. Micro-averaged F1 denotes the F1 measured from all instances and is sensitive to the skew in the distribution of classes in the dataset.

B Additional Classifier Results

<table>
<thead>
<tr>
<th></th>
<th>Baseline</th>
<th>Self Tweets</th>
<th>Friend Tweets</th>
<th>Directed Tweets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>52.0</td>
<td>68.4</td>
<td>75.2</td>
<td>70.4</td>
</tr>
<tr>
<td>Religion</td>
<td>66.2</td>
<td>9.7</td>
<td>71.5</td>
<td>25.9</td>
</tr>
<tr>
<td>Diet</td>
<td>51.3</td>
<td>17.0</td>
<td>55.7</td>
<td>31.2</td>
</tr>
<tr>
<td>Extroversion</td>
<td>64.8</td>
<td>78.7</td>
<td>65.3</td>
<td>78.7</td>
</tr>
</tbody>
</table>

Table 4. Predictive accuracy for categorical attributes, reported as Micro-F1 and Macro-F1.

<table>
<thead>
<tr>
<th></th>
<th>Baseline</th>
<th>Self Tweets</th>
<th>Friend Tweets</th>
<th>Directed Tweets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>38.1</td>
<td>0.00</td>
<td>17.2</td>
<td>0.27</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>20.7</td>
<td>0.26</td>
</tr>
</tbody>
</table>

Table 5. Predictive accuracy for age, reported Mean Squared Error and Correlation.

C Additional Measures of Tie Strength

We initially considered two other potential proxies for tie strength based on textual analysis. First, we replicated the approach of Gilbert and Karahalios [44] which counted words occurring in ten LIWC categories to approximate intimacy in communication. Second, we attempted to measure social distance [58] by drawing upon Construal Theory [59, 110] which conjectures that individuals with low social distance typically use more concrete language, whereas those with high social distance use more abstract language [99, 98]; here, communication concreteness was measured using the word concreteness ratings of [16]. However, we found that the ratings for each approach did not match our judgments for their respective intended attributes and their use in the regression models produced non-significant results. Without ground truth for intimacy and social distance to validate their ratings, we therefore omitted these proxies based on our judgment of their unreliability to avoid drawing false conclusions about these dimensions of tie strength.
References

48. Granovetter, M.S.: The strength of weak ties. American journal of sociology 78(6), 1360–1380 (1973)
89. Reed, P.J., Spito, E.S., Butts, C.T.: Thumbs up for privacy?: Differences in online self-disclosure behavior across national cultures. Social science research 59, 155–170 (2016)