Online Social Network Inference Attacks State-of-Art Overview

Anna Bonaldo
student ID 1154780

Abstract—
Social media platforms allows users to share their personal informations and opinions and to follow other users ones. In recent years such kind of platform number has increase and for the most popular sites even the number of user has increase in a sensitive manner. As result, today On-line Social Networks (OSN) groups lot of information about people, communities and their behaviour, preferences, connections and location. In last few years some works show that user personal attributes and also other sensitive data can be inferred from on public available informations. This work focus on inference methods, purposing a review of at present day state-of-art and discussing about techniques' effectiveness and possibles improvements. We, otherwise, leave apart the question on of how we can prevent information inference attacks.

Index Terms—privacy leakage, information inference, attributes inference, OSN, online social networks, inference attaks, multiple profiles identification.

1 Introduction

Many recent works focus on information inference from OSN. In following paragraph we will summarize main past approaches' features. First of all, we bring a brief overview on information has been shown we can infer form OSNs and what input information past techniques start from to infer it.

1.1 What information can we infer?

Main sensitive data categories we get as inference output are:

- **Personal attributes** name, age, gender, geographical informations like location, nationality, language, city and education (details in 1.2).
- **Advanced personal attributes**: credit profiling (datails in 2.1) , political preferences, occupation.
- **Identity linking between profiles on different OSN.** details in 3.
- **Health and psychological information** : personality traits, weight, height, mental illness presence 2.3,2.4.

1.2 What information can we start form?

Before discussing all techniques in a detailed manner, we want to summarize input information inference method need to perform inference process correctly.

- **Public profile's attributes (Pub.Attr)**: publicly available profile descriptions on preferences, name, age, school, city,etc.
- **Social Graph(SGraph)** Number of friends, friends list and attributes [6, 7, 14].
- **Behavioural data**: page liking or re-posting percentage, posting time and frequency [20, 28].
- **Text input** like user status, descriptions, public statements.
- **Natural Language style features (NLP)** [1]
- **Profile photos (Img)** [24, 9, 8, 10, 16]
- **Other information** Amazon wish list, etc. [], 26].

Section 2 lists out, in a more detailed way, advanced information inference approaches while 3 discuss on method for users profiles' **identity linking** between multiple OSN. Some consideration will be done in 4 about applied method and algorithm and their effectiveness. We will then purpose some possible improvement on presented techniques.

2 Sensitive attribute disclosure

User attributes are usually considered in information security and privacy laws as Personally identifiable information (PII). *Quasi-identifiers* are instead private attributes that are not of themselves unique identifiers, but are sufficiently well correlated with an entity that they can be combined with other quasi-identifiers to create a unique identifier. It has been shown they can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context[19]. Many inference technique to infer such kind of information has been

Attribute	Work	Year	Accuracy	Method	OSN	Inference Input
Gender						
	[26]	2017	-	Inference from first name	Amazon	User first Names
	[14]	2015	95.70	Graph Label Propagation (GLP)	Pokec	SGraph
	[14]	2015	91.60	Graph Label Propagation (GLP)	Facebook	Social Graph
Age						
minor/major[1]	[14]	2015	55.20	Graph Label Propagation (GLP)	Facebook	SGraph, PubAttr
	[14]	2015	2.2[2]	Graph Label Propagation (GLP)	Pokec	SGraph, PubAttr
Location						
160km	[12]	2010	51.00	Probabilistic (ML)	Twitter	Text: geo-tags
State level	[15]	2010	24.00	Geographic topic model (NLP)	Twitter	NLP[3],Text: geo-tags
Zip code level	[23]	2011	13.90	Language Models	Twitter	Text: geo-tags
Town level	[23]	2011	24.80	Language Models	Twitter	Text: geo-tags
160km	[11]	2012	49.90	Gaussian Mixture models and MLE (ML)	Twitter	Text:geo-tags
160km	[25]	2012	62.30	Probabilistic (ML)	Twitter	SGraph
10km	[21]	2012	20.00	Machine Learning	Twitter	Text:geo-tags
10km	[32]	2013	37.00	Gazzetteer	Twitter	NLP, geo-text composition
10km	[30]	2014	60.00	Probabilistic (ML)	Twitter	NLP
0,1km	[31]	2012	57.00	Dynamic Bayesian Networks	Twitter	Imgs, Text:geo-text
Country level	[29]	2017	95. 81	Multinomial Log. Regr., Deep L.	Twitter	Text:geo-tags
City level	[29]	2017	59.20	Multinomial Log. Regr,Deep L.	Twitter	Text:geo-tags
City level	[29]	2017	70.34	Multinomial Log. Regr,Deep L.	Weibo	Text:geo-tags
City level	[13]	2011	88.60	Graph Label Propagation (GLP)	Facebook	
City level	[29]	2017	91.52	Multinomial Log. Regr,Deep L.	Facebook	Text: locality tags
Language [4]						
	[14]	2015	80.42	Graph Label Propagation (GLP)	Pokec	SGraph, PubAttr
Habits,Education:						
Driker	[14]	2015	65.42	Graph Label Propagation (GLP)	Pokec	SGraph, PubAttr
Smoker	[14]	2015	71.65	Graph Label Propagation (GLP)	Pokec	SGraph, PubAttr
Music [5]	[14]	2015	73.09	Graph Label Propagation (GLP)	Pokec	SGraph, PubAttr,
Education	[7, 6]	2016, 2017	75.00	Graph Label Propagation (GLP)		SGraph, PubAttr
Education	[14]	2015	16.70	Graph Label Propagation (GLP)	Facebook	SGraph, PubAttr

presented in works in 1.2. High accuracy techniques are available for basic information, especially gender and age. But also location, education language and habits can be decided with good accuracy results from highly available data. Recent works show that also more complex and sensitive information can be inferred from OSN profiles. Most relevant results have been summarized in following lines.

2.1 Credit profile inference

User credit is a particularly private attribute, usually more sensitive than age or gender in most cases. Users seldom generate credit related personal data on the social web. Consequently, social data only contains extremely weak signals about user credit risk [20]. Work in [20], based on Twitter platform, perform an analysis on behavioural data that are usually more precise and formal than tweets content itself, and reflects users' behaviour habits and characters more comprehensively and directly.

Credit profiling task has been performed in [20] using standard l2-regularized logistic regression classifier whose input is the latent user behaviour dimensions. After the classifier learning phase, they could distinguish behaviour dimensions that are informative for credit prediction from the classifier easily. Their experiments achieve an accuracy around 63.5% in predicting credit profiles on available data.

2.2 Overweight status inference

Work in [24] uses a computer-vision approach to make an evaluation of user body mass index using profile images. Profiles' pictures are available in most cases for OSN profiles, even for more popular social platforms. Inferring basic attributes from them is considered as a privacy attack, but we can assume that getting health information from a so far available resource should be considered a more serious privacy issue. The considered work starts form a dataset of 4206 faces photos collected on Reddit. The experiments aims to distinguish between some BMI (Body Mass Index) ranges that are: [16.0 -18.5], [18.5-25],[25-30], [30-35], [35-40], [$\geq$40]. Male-female subdivision in photo dataset was of 2438 males and 1768 females. For training phase 3368 images where used, while 838 were implied in testing phase. Results show **accuracy value of 71% for male face BMI classification and of 57% for female BMI classification**, considering the most performing version of purposed algorithms. As last phases of the study, the same classification

task over here has been submitted to humans. Then accuracy results have be compared. The accuracy difference between human and machine performances were really similar. Humans outperforms machines in most cases, but with a greater accuracy of at most 5%.

2.3 Inference on mental-health conditions

In [3] authors develop neural MTL models for prediction tasks on users' mental health status. They work on 10 classification task: 8 on mental health conditions, one on neurotypicality presence and gender classification. Considered mental health condition are: neurotypicality, anxiety, depression, suicide attempt, eating disorder, schizophrenia, panic disorder, bipolar disorder, PTSD. The total training set size was about 9611 users, divided as 788 males and 248 females. They opt for a neural architecture to exploit the synergies between mental conditions. They chose a model that allow to get improvements over single task models by using MTL (Multiple Task Learning) that is predicting multiple related tasks and that allow to exploit any correlations between the predictions. MTL model performance was compared with STL (Single Task Learning) models to predict each task independently. Results show that the most complex MTL model performs significantly better than independent LR models, reaching 0.846 for TPR[6] and FPR[7] of 0.1. Choosing the correct set of auxiliary tasks for a given mental condition can yield a significantly more predictive model. The MTL model used in this work seems to be really helpful in improving performance for training with small amount of data. We can see that in STL case the performances are badly affected for small training dataset. Otherwise MTL give better performances even for categories with really low number of training examples. AUC (Area Under Curve) measure shows an good performance on tasks, but it is not really high (they get at most a TPR = 0.81). Otherwise we should consider that this is not a simple classification task and, with that point ov view, we should consider this a really hopeful inference result. What not seems so clear is kind of input data experiment uses. They say they uses all uses history on Twitter, but no implementation detail is given. As reported, the relative frequency of the 5 000 most frequent n-gram features, for $n \in 1, 2, 3, 4, 5$ in data,has been computed and then feed as input to all models. Otherwise, this procedure seems to be a core feature for successful implementation, and is difficult to analyse in presence of no other information.

6. True Positive Rate
7. False Positive Rate

2.4 Personality traits inference

A work in[34] tries to understand if profile pictures contain information about their owners' personality. They found the amount of significant correlations found was considerable, which supports the previous other works findings that personality traits have an influence on the choice of profile pictures in Facebook. Multiple feature extraction has been executed for tree main features categories:colour, composition and textural properties. They apply different systems to perform features extraction such as Computational Aesthetics (CA), Convolutional Neural Networks(CNN) and other two feature extraction systems that are IATO [8] and Pyramid Histogram Of visual Words based features. Best accuracy in features extraction task were obtained combining all experimented methods together and is of **60% for all 5 personality profile considered.** A later work on personality feature extraction from images of social networks profiles that uses a similar 5-grade personality classification model get better results in classification of profiles. Achieved accuracy improves previous results of a percentage that starts from +0.8% up to +15%. Result in [8, 34] where again outperformed by [10] that develops a complex framework for personality classification using social media data. They has developed a profiling technology that perform prediction for customers profiling for advertising customization scopes. Their product is based on different sources of digital footprints (e.g. images, textual contents, demographics, social media activities, etc.), and is able to predict a set of behavioural variables, including purchase motivations, job performance and subjective well-being. They underline the importance of exploiting public information and using mixed typologies of data sources. They refer their system reach an accuracy of 80% in predicting personality traits. Even other recent works [16] exploit personality prediction from social media data for services customization, enforcing that effectively predicting personality traits is today a feasible task. In particular work in [5] reports accuracy value achieved for personality traits prediction, comparing accuracy for predictions on single OSN data and multiple OSN data. From their results we can see that using multiple source of data increase in a sensible way accuracy of predictions. Otherwise they point out that it is not always true that the more data we get, the more is the accuracy. Their experiments results shows that in each experiment set-up, pairs of OSN data association always outperform tree-OSN data association.

3 IDENTITY LINKING

Users have today identities across several social computing systems and reveal different aspects of their

lives in each. This enlarges considerably the scope of information disclosure [2]. We will call this inference attacks *identity linking (IL)*. This technique is really powerful because users reveal different pieces of information on different social computing systems (e.g., personal life on Facebook, profession on LinkedIn, interests on Twitter) [2, 22]. In 2011 work in [22] shows that identity linking can highly increase deanonymization risk, allowing attacks like password recovering throw gained users' personal informations.

A recent 2017 study [26] shows that personal quasi-identifier'[8] like age, gender and name are often available for Amazon profiles. Amazon wish lists visibility can be set as private. Otherwise public visibility is the default setting and many users chooses to left it public (or maybe forget to change list visibility). This study shows that information on users expenses can be collected from Amazon users profiles. Also other information about users relatives and habits emerge from descriptions and items informations. For more classical OSN platforms, such information can be inferred only with highly advanced method and with lower precision (see for example credit profile prediction in [20] commented in 2.1).

For this reason working on multiple OSN profile connection seems to be a really powerful approach, that exposes users to high privacy leakage risks.

Traditionally, identity linking and relative attributes disclosure risks have been quantified through k-anonymity. A recent study cited by [2] proposed to adapt k-anonymity by considering two identities as indistinguishable if they are similar enough (rather than having the same quasi-identifiers) – thus define k-anonymity in social computing systems as the number of identities in T that are similar enough with I_T . Authors in [2] purpose to extend k-anonymity into the concept of "matching anonymity ". Their aims was not performing identity disclosure itself, but analyse risk of information leakage correlated with this techniques. Otherwise, they point out some relevant issue on this topic that are:

• Probabilistic approaches often outperform exact methods.

• Traditional entity similarity measure must be adapted to OSN scope. They purposes a new similarity measure that quantifies the probability of two identities to belong to the same user.

• Only if attributes are available, identities matching is feasible with high accuracy. Otherwise, for missing information, performing the task correctly become infeasible.

A more pragmatic approach is presented in [28]. They propose the use of automated classifiers to classify the input profiles as belonging to the same user or not. Users informations for each social system profile were systematized into feature vector then compared in pairs to generate similarity vector between OSNs' profiles. Similarity measures where computed with custom-field metrics. Discriminative capacity of each metric was also evaluated with different approaches. Accounts where collected from Twitter and LinkedIn to produce a training set for the classifiers. They perform supervised training with following classifiers: Naive Bayes, k-nearest-neighbours, Decision Tree and Support Vector Machines. Results were really promising: they reach accuracy of 98% for the best classifiers (Naive Bayes) and also high accuracy for classification with decision tree and SMV (96.5%, 97%).

8. **Quasi-id**: Non-unique identifies that have been shown to be linkable to unique identities

4 What can we learn form state-of-art review?

4.1 Inference algorithms

Analysing reviewed works, we see different algorithms works better in diverse conditions. **Multi-task learning** works better [3] because it exploits information in a more efficient way. Otherwise **Graph Label Propagation** approach perform better for basic attributes and has the advantage it does not require training, differently form supervised ML approaches. **Machine Learning (ML)** approaches get better results for advanced attributes and inference on behavioural data [20, 29, 1]. Additionally, distinguishing between target attributes types can improve inference accuracy[14]. We observe that in some cases, improvement in training dataset size and target classification values could bring to better accuracy (for example in [24]).

4.2 Public information only!

Inference methods should exploit only public information. Because only few public information can be available in many cases, most efficient techniques uses all available information they can access. Many valid approaches cannot reach high accuracy probably because they lie only on few public values like [14]. Many approached we listed lie on dataset information. Feasibility of inference attack should lay on real cowled data, because they could perform differently from datasets [17]. Otherwise some ML method need a training set, in the beginning. Otherwise, training and set should be chosen in reality-consistent way, to support attack feasibility.

4.3 Different target OSNs

Many approaches have been purposed on different OSN. Approaches on a OSN can be hardly reproduced in another one, especially for OSN with different structure or content type. For example Twitter has a different structure from Facebook or Instagram. **No combination methods have been presented.** Few works focus on combining all methods we know for information inference to get a full description of users profiles. Most of cited method focus on precise inference of one or few attributes, but none, even for identity linking papers, works on build a complete user profile with inference techniques. Information inference is more effective the more is information we know about users, and the more accuracy we have on its reliability.So, in following section we describe some improvements of this techniques, that lays on combination of multiple past results, to get a complete user profiling.

5 Full profile inference

In most cases, we have more available techniques to infer the same attributes. What we can do, to allow complex attacks on OSN profiles, is simply choose the easiest way to infer each attribute from available information. As example, if we want to infer gender for a OSN profile, first of all we should simply try to classify user complete name as common female or male name. Only if this approach fails on real data, we should try more advanced techniques. The main reason for this approach is not only efficiency, but also accuracy and interpretability.

5.1 Combining inferred data

Available techniques for attribute inference lay often on different input informations. So, we can combine them to get higher accuracy on attribute value estimation, without introducing bias in our data. As suggested by [14], distinguish between attribute type guarantees higher performance. So we purpose custom approaches for each attribute type. For **numerical values** averaging all values is the easiest way to combine such kind of information. Weighted averaging is also recommendable for different accuracy scores know each approach we use has reach in testing phases. For non-finite subset of target values, we should try at first to reduce the problem to a classification (or multi-value classification) problem. This has been shown to be really effective for complex users attributes in [9, 3, 10]. We know that for classification methods output is usually more reliable for small target set of **categorical values**. So we suggest to reduce as is possible attribute it. For complex classification problems, like location inference, we suggest a multilayer classification that ar each step tries to refine information of the previous one. In table 1.2 different grain approaches are listed. For example we should infer language from text as first, then refine with country, then region or city. This improves attack effectiveness and also let the attacker choosing the most effective inference method at each step. Identity disclosure bring higher information on users to the attacher, as has been shown by [22]. Otherwise sometimes we does not have sufficient information to an effective cross social system attacks. In this situations we could enrich available information using attribute disclosure attacks on missing fields. In creating a framework for complete-profile inference, we should put our effort only on missing information, and apply the most efficient method to infer the missing one.This because, as previously said, simplicity and efficiency join with accuracy in most cases. We should remember that if we use previously inferred information as input of other inference process we should rely only on "almost-certain" informations. If some inference method has been shown to have low accuracy on test sessions, we should not use such kind of information as input of new inference processes. Otherwise this could bring bias and errors in our computation.

5.2 Statistical approach to Identity Disclosure

Cross social system identity disclosure is a computational expensive task. Additionally we're not certain about users' presence on other OSNs, and we could fail in finding additional information. Otherwise, OSN are not all equivalent: they differs for kind of users, their age, their nationality, language, social extraction, etc. Lot of data have been collected throw the years on this aspects by statistical survey but also by OSN providers. For this reason, once we know some basic attributes for each users, we could extend our search on other OSN basically choosing the most suitable for each user category. As an easy example, trying to discovering more information starting by a set of Facebook users, we probably fail searching on LinkedIn profiles matching for under-18 users. In this case we could split the search by users age, targeting LinkedIn for over-18 users and Instagram for the other. Another approach is starting from OSN that are more popular on the web, and proceed at each step to more popular ones. While it is likely probable that a user with a profile on LinkedIn has a profile on Facebook, the converse has lower probability. This is simply because Facebook number of users at present date 2167 M users while LinkedIn has today 260 M users [27]. We can use some expedient to improve identity linking efficiency. For example we can collect

statistical data on target OSN, with information on users age, country, language, etc. Then, for each OSN we want perform IL on, we should determine the main probable user class in it. With user available attributes' information in this step, we can perform, for starting OSN, a users' classification based on classes we'have previously estimated for others OSN. We then proceed with IL only for selected user subset for each OSN. This method need cross OSN inference technologies. Otherwise, it aims to maximize finding probability on entire user set. As a consequence, even attribute accuracy should be maximized with this approach. Even if repeated multiple times, with different OSN, it leads to maximization of IL probability. This improves techniques performaces, while identity linking is an expensive task.

6 Conclusions

Information inference is a recent attack that exploits OSN vulnerabilities and last years machine learning methods growth. We can conclude, from collected results, that inference accuracy is growing fast on our days and will rely in following year on more articulated and accessible inference frameworks.

Appendix

Here we insert some pseudo-code make previously discussed approaches more clear and detailed.

Procedure 1: accuracy refinement on multiple OSNs.

```
Data:= [];
//Initialize OSNset
OSNset:= [Facebook, LinkedIn, ..];
Order OSNset from lower to higher
  probability to find users;
//result:  OSNset = [LinkedIn,..,
    Facebook]

For each i-OSN in OSNset: {
 For each user in OSN: {
   Public-i =  i-OSN public attribute;
     Data = Data + Public-i;
     Infer();
     MergeData(); }}
```

Procedure 2: attribute inference on single OSN

```
Infer(){
For each user profile in OSN: {
 Public = [OSN public attribute];
 Estimate "least-missing-fields"  Public;
 Order Public in decreasing
  "least-missing-fields" number;

 // BASIC
 For each missing attribute:{
    InferAttribute();
 }

 //ADVANCED REFINEMENT
 For each user profile in OSN: {
   For each missing attribute:{
      // value refinement
      InferFromBehavioural();
    } }
}
```

Procedure 3: merge multiple attributes' values

```
MergeData(){
 For each user:
   For each attribute: {
      Type-Taylored-Merge();
      // Custom merge for each attr. type
   }}}
```

References

[1] Oluwaseun Ajao, Jun Hong, and Weiru Liu. "A survey of location inference techniques on Twitter". In: *Journal of Information Science* 41.6 (2015), pp. 855–864.

[2] Athanasios Andreou, Oana Goga, and Patrick Loiseau. "Identity vs. Attribute Disclosure Risks for Users with Multiple Social Profiles". In: *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017*. ACM. 2017, pp. 163–170.

[3] Adrian Benton, Margaret Mitchell, and Dirk Hovy. "Multitask learning for mental health conditions with limited social media data". In: *Proceedings of the 15th Conference of the EACL*. Vol. 1. 2017, pp. 152–162.

[4] Andrea Burattin, Giuseppe Cascavilla, and Mauro Conti. "Socialspy: Browsing (supposedly) hidden information in online social networks". In: *International Conference on Risks and Security of Internet and Systems*. Springer. 2014, pp. 83–99.

[5] Kseniya Buraya et al. "Towards User Personality Profiling from Multiple Social Networks." In: *AAAI*. 2017, pp. 4909–4910.

[6] Giuseppe Cascavilla et al. "OSSINT-Open Source Social Network Intelligence An efficient and effective way to uncover" private" information in OSN profiles". In: *arXiv preprint arXiv:1611.06737* (2016).

[7] Giuseppe Cascavilla et al. "Revealing censored information through comments and commenters in online social networks". In: *Advances in Social Networks Analysis and Mining (ASONAM), 2015 IEEE/ACM International Conference on*. IEEE. 2015, pp. 675–680.

[8] Fabio Celli. *IATO: Feature Extraction for image analysis*. Tech. rep. Technical Report. University of Trento, 2015.

[9] Fabio Celli, Elia Bruni, and Bruno Lepri. "Automatic personality and interaction style recognition from facebook profile pictures". In: *Proceedings of the 22nd ACM international conference on Multimedia*. ACM. 2014, pp. 1101–1104.

[10] Fabio Celli, Pietro Zani Massani, and Bruno Lepri. "Profilio: Psychometric Profiling to Boost Social Media Advertising". In: *Proceedings of the 2017 ACM on Multimedia Conference*. ACM. 2017, pp. 546–550.

[11] Hau-wen Chang et al. "@ Phillies tweeting from Philly? Predicting Twitter user locations with spatial word usage". In: *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012)*. IEEE Computer Society. 2012, pp. 111–118.

[12] Zhiyuan Cheng, James Caverlee, and Kyumin Lee. "You are where you tweet: a content-based approach to geo-locating twitter users". In: *Proceedings of the 19th ACM international conference on Information and knowledge management*. ACM. 2010, pp. 759–768.

[13] Clodoveu A Davis Jr et al. "Inferring the location of twitter messages based on user relationships". In: *Transactions in GIS* 15.6 (2011), pp. 735–751.

[14] Raïssa Yapan Dougnon, Philippe Fournier-Viger, and Roger Nkambou. "Inferring user profiles in online social networks using a partial social graph". In: *Canadian Conference on Artificial Intelligence*. Springer. 2015, pp. 84–99.

[15] Jacob Eisenstein et al. "A latent variable model for geographic lexical variation". In: *Proceedings of the 2010 Conference on Empirical Methods in Natural Language Processing*. Association for Computational Linguistics. 2010, pp. 1277–1287.

[16] Francesco Gelli et al. "How Personality Affects our Likes: Towards a Better Understanding of Actionable Images". In: *Proceedings of the 2017 ACM on Multimedia Conference*. ACM. 2017, pp. 1828–1837.

[17] Oana Goga et al. "On the reliability of profile matching across large online social networks". In: *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM. 2015, pp. 1799–1808.

[18] Neil Zhenqiang Gong and Bin Liu. "You Are Who You Know and How You Behave: Attribute Inference Attacks via Users' Social Friends and Behaviors." In: *USENIX Security Symposium*. 2016, pp. 979–995.

[19] Sari Stern Greene. *Security Program and Policies: Principles and Practices*. Pearson IT Certification, 2014.

[20] Guangming Guo et al. "Personal credit profiling via latent user behavior dimensions on social media". In: *Pacific-Asia Conference on Knowledge Discovery and Data Mining*. Springer. 2016, pp. 130–142.

[21] Yohei Ikawa, Miki Enoki, and Michiaki Tatsubori. "Location inference using microblog messages". In: *Proceedings of the 21st International Conference on World Wide Web*. ACM. 2012, pp. 687–690.

[22] Danesh Irani et al. "Modeling unintended personal-information leakage from multiple online social networks". In: *IEEE Internet Computing* 15.3 (2011), pp. 13–19.

[23] Sheila Kinsella, Vanessa Murdock, and Neil O'Hare. "I'm eating a sandwich in Glasgow: modeling locations with tweets". In: *Proceedings of the 3rd international workshop on Search and mining user-generated contents*. ACM. 2011, pp. 61–68.

[24] Enes Kocabey et al. "Face-to-bmi: Using computer vision to infer body mass index on social media". In: *arXiv preprint arXiv:1703.03156* (2017).

[25] Rui Li et al. "Towards social user profiling: unified and discriminative influence model for inferring home locations". In: *Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM. 2012, pp. 1023–1031.

[26] Yue Li et al. "A measurement study on Amazon wishlist and its privacy exposure". In: *Communications (ICC), 2017 IEEE International Conference on*. IEEE. 2017, pp. 1–7.

[27] MultiMedia LLC. *We Are Social. "Most Popular Social Networks Worldwide*. 2018. URL: www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (visited on 02/03/2018).

[28] Anshu Malhotra et al. "Studying user footprints in different online social networks". In: *Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on*. IEEE. 2012, pp. 1065–1070.

[29] Yujie Qian et al. "A Probabilistic Framework for Location Inference from Social Media". In: *arXiv preprint arXiv:1702.07281* (2017).

[30] KyoungMin Ryoo and Sue Moon. "Inferring twitter user locations with 10 km accuracy". In: *Proceedings of the 23rd International Conference on World Wide Web*. ACM. 2014, pp. 643–648.

[31] Adam Sadilek, Henry Kautz, and Jeffrey P Bigham. "Finding your friends and following them to where you are". In: *Proceedings of the fifth ACM international conference on Web search and data mining*. ACM. 2012, pp. 723–732.

[32] Axel Schulz et al. "A Multi-Indicator Approach for Geolocalization of Tweets." In: *ICWSM*. 2013, pp. 573–582.

[33] H Andrew Schwartz et al. "Personality, gender, and age in the language of social media: The open-vocabulary approach". In: *PloS one* 8.9 (2013), e73791.

[34] Cristina Segalin et al. "What your Facebook profile picture reveals about your personality". In: *Proceedings of the 2017 ACM on Multimedia Conference*. ACM. 2017, pp. 460–468.