LEARNING PRIVATE REPRESENTATIONS WITH FOCAL ENTROPY

Anonymous authors
Paper under double-blind review

ABSTRACT

How can we learn a representation with good predictive power while preserving user privacy? We present an adversarial representation learning method to sanitize sensitive content from the representation in an adversarial fashion. Specifically, we propose *focal entropy* - a variant of entropy embedded in an adversarial representation learning setting to leverage privacy sanitization. *Focal entropy* enforces maximum uncertainty in terms of confusion on the subset of privacy-related similar classes, separated from the dissimilar ones. As such, our proposed sanitization method yields deep sanitization of private features, yet is conceptually simple and empirically powerful. We showcase feasibility in terms of classification of facial attributes and identity on the CelebA dataset as well as CIFAR-100. The results suggest that private components can be removed reliably.

1 INTRODUCTION

Lately, the topics of privacy and security are enjoying increased interest in the machine learning community. This can largely be attributed to the success of big data in conjunction with deep learning and the urge to create and process ever-larger data sets for mining. However, with the emergence of more and more machine learning services becoming part of our daily lives and making use of our data, special measures must be taken to protect the privacy and decrease the risk of privacy creep Narayanan & Shmatikov (2006); Backstrom et al. (2007). Simultaneously, growing privacy concerns entail the risk of becoming a major deterrent in the widespread adoption of machine learning and the attainment of their concomitant benefits. Therefore, reliable and accurate privacy-preserving methodologies are needed, which is why the topic lately has enjoyed increased attention in the research community.

Several efforts have been made in machine learning to develop algorithms that preserve user privacy while achieving reasonable predictive power. Solutions proposed for privacy in the research community are versatile. A standard approach to address privacy issues in the client-server setup is to anonymize the *data* of clients. This is often achieved by directly obfuscating the private part(s) of the data and/or adding random noise to raw data. Consequently, the noise level controls the trade-off between predictive quality and user privacy (e.g., data-level Differential Privacy Dwork (2006)). These approaches associate a privacy budget with all operations on the dataset. However, complex training procedures run the risk of exhausting the budget before convergence. A recent solution to such a problem has been federated learning McMahan et al. (2016); Geyer et al. (2017), which allows us to collaboratively train a centralized model while keeping the training data decentralized. The idea behind this strategy is that clients transfer the *parameters* of the training model in the form of gradient updates to a server instead of the data itself. While such an approach is appealing to train a network with data hosted on different clients, transferring the models between clients and server, and averaging the gradients across the clients generates significant data transmission and extra computations, which considerably prolongs training. Another widely adopted solution is to rely on encoded data *representation*. Following this notion, instead of transferring the client's data, a feature representation is learned on the clients' side and transferred to the server. Unfortunately, the learned features may still contain rich information, which can breach user privacy Osia et al. (2017; 2018). Also, the extracted features can be exploited by an attacker to infer private attributes Salem et al. (2019). Yet, another approach is homomorphic encryption Armknecht et al. (2015). Despite providing strong cryptographic guarantees, in theory, it incurs considerable computational overhead, which still prevents its applicability for SOTA deep learning architectures Srivastava et al. (2019)

The recent success of adversarial learning in making the representations fair Louizos et al. (2015), unbiased Madras et al. (2018), and controllably invariant to sensitive attributes Xie et al. (2017), has led to the increased adoption of Adversarial Representation Learning (ARL) to control the private information encapsulated within the representation Roy & Boddeti (2019); Sadeghi et al. (2019). In the common ARL formalization of the privacy-preserving representation learning, a "predictor" seeks to extract the desired target attributes while an "adversary" seeks to reveal the private attributes. However, the solutions mentioned earlier can only meet its practical promises when the private attributes do not strongly correlate with the target attributes. In this paper, we deal with adversarial privacy-preserving representation learning in the presence of highly overlapping information. In this setting, the target and sensitive attributes are related to each other (e.g., beard and gender) to a large extent. The objective of this task is to learn a representation that contains all the information about non-sensitive attributes. At the same time, it omits to encode the sensitive attributes of them. Such representation can be transmitted to the server without concerns regarding the privacy revelation of classifiers having equal and higher capacity than the adversarial proxy used during training. For that, we adopt an ARL procedure and propose to learn a representation which maximizes the likelihood of the target information (i.e., *attribute predictor*), while increasing the uncertainty about the class that each sample belongs to (i.e., *class adversary*). With that, we intuitively tie the privacy notion to the class-level information and sanitize the class-revealing information from the representation in a semantic-aware fashion.

Specifically, we propose to learn the representation using the popular Variational Autoencoders (VAE) Kingma & Welling (2013), where the latent representation is additionally decomposed into two latent factors: *target* and *residual*. Whereas the target part encodes the information for the target task, the residual part identifies and collects the data's private part. In order to sanitize the target representation, we leverage an ARL procedure. There are two general strategies for ARL: the common solution for adversarial optimization is to maximize the loss of the adversary by minimizing the negative log-likelihood of sensitive variables. However, this is practically sub-optimal from the perspective of preventing information leakage. If the optimization does not reach the equilibrium, the resulting distribution associated with the minimum likelihood solution is subject to leaking the most amount of information. Another solution for adversarial optimization is to maximize the adversary's entropy by enforcing a uniform distribution over the sensitive labels Roy & Boddeti (2019); Sarhan et al. (2020). Such a solution provides no information to the adversary. However, it has the risk of weakening the encoder as it partially eliminates the role of the adversary in the representation learning phase and is provably bound to the adversary's optimality.

To combine the best of both worlds, we propose to maximize a variant of entropy - *focal entropy* - for dealing with inter-class uncertainty maximization. Focal entropy enforces the uncertainty to focus on a sparse set of similar classes and prevents the vast number of dissimilar classes from overwhelming the uncertainty. Maximization of focal entropy increases the uncertainty in a more organic fashion, leading to a deeper privacy sanitization during the representation learning phase.

In summary, the main contributions of this paper are three-fold. **First**, we propose to learn the privacy-preserving representations in the presence of highly overlapping information between the target and sensitive attributes. **Second**, we introduce an ARL setting for this task by adding a novel entropy term to the VAE. **Third**, we demonstrate experimentally that our proposed method learns a semantically meaningful privacy-preserving sanitized representation.

2 Related Works

Much research has been conducted in protecting differential privacy Dwork et al. (2017); Dwork (2006); Ryoo et al. (2017); Abadi et al. (2016) on *data* and *parameter* level by anonymizing raw data directly, or incorporating a randomized mechanism into the learning process, respectively. Although successful, our method is fundamentally different from them, as we aim to learn a private representation instead of preserving privacy in *data* or *parameter* level. While we do not consider their framework here, our method could employ differential privacy during the post-classifier training.

The advantages of learning and transmitting *representations* instead of data have been investigated recently in many works, see Osia et al. (2017; 2018), and references therein. Nevertheless, such a representation is proven to contain some privacy revealing information of clients. The recent success of adversarial learning has led to the increased adoption of this technique for learning

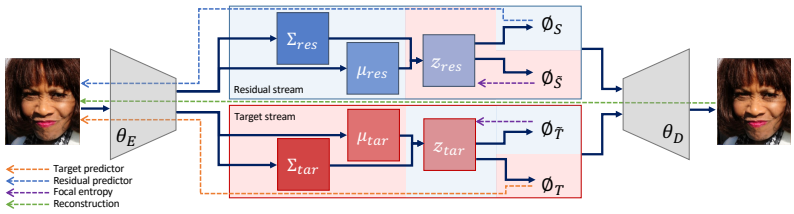


Figure 1: **Our proposed architecture:** the two stream network is based on VAE, and augmented with additional predictor loss and (focal) entropy.

representations that preserve sensitive information in different types of data. For instance, Srivastava et al. (2019) proposed to learn privacy-preserving representations for automatic speech recognition (ASR). In Yang et al. (2018), a representation is learned on the raw student clickstream event data, captured as they watch lecture videos in massive open online courses. In Li et al. (2019), the authors proposed an obfuscator designed to hide privacy-related sensitive information from the features using adversarial training. Similarly, Kim et al. (2019) is based on adversarial learning, which encodes images to obfuscate the patient identity while preserving enough information for a medical segmentation task. Pittaluga et al. (2019) considered a formulation based on adversarial optimization between the encoding function and estimators for private tasks. Although our method is also based on adversarial learning, we differently facilitate adversarial sanitization using entropy. This leads to a more privacy-preserving representation while maintaining the method complexity.

The most related work to ours is by Roy & Boddeti (2019); Sadeghi et al. (2019), which aims at obtaining a sanitized representation using entropy and adversarial representation learning, respectively. Another related work to our paper proposed by Feutry et al. (2018) aims at learning representations that preserve the relevant part of the information while dismissing information about the private labels corresponding to the clients' identity. A key difference compared to this method is that they require labels for the downstream task during representation learning. Recently, Chen et al. (2018) proposed a complex method for privacy-preserving representation learning. Gabbay & Hoshen (2020) propose an approach for disentanglement using shared latent optimization and an asymmetric regularization. Edwards & Storkey (2016) propose sanitize representations utilizing an adversary. Liao et al. (2019a;b) employ an adversary to obtain a sanitized representation, however, also incorporating fairness constraints. Liu et al. (2018) proposed to use conventional entropy an adversary in the context of a vanilla auto-encoder for privacy sanitization. To the best of our knowledge, our paper is the first work that proposes to taking the class similarity into account for the entropy of the adversary. Furthermore, fairness as proposed in Creager et al. (2019); Locatello et al. (2019); Quadrianto et al. (2019); Sarhan et al. (2020) is yet another intimately connected notion to privacy. While we do not consider fairness here, our method could also be extended to that problem, leading to exciting future research. Finally, we note that our model is different from the federated learning methodology in McMahan et al. (2016); Geyer et al. (2017), which focuses on learning a decentralized private model by sharing gradient updates instead of learning representations.

3 METHOD

We consider the scenario where we want to learn a dual-objective feature representation. The first objective entails providing high accuracy in terms of target attribute classification. The second objective entails minimizing information leakage w.r.t. sensitive attributes, ideally making classification impossible. To this end, we learn an encoder that channels the information by decomposing the representation into two parts: target and residual partition. The target partition allows classification for the target attributes and is sanitized w.r.t. the sensitive attributes. In contrast, the residual partition captures the information w.r.t. the sensitive attribute, subsuming the excess information. To drive the representation learning, we employ a Variational Auto-Encoder (VAE) Kingma & Welling (2013). Isolating information about sensitive and non-sensitive attributes to separate subspaces then corresponds to integrating the VAE into a minimax game between the target classifiers and the adversary.

Background: The representation learning problem is formulated as a game among *six* players: an Encoder E, a decoder D, a target predictor T, a sensitive attribute predictor S, two adversarial

classifiers $\tilde{T}$, $\tilde{S}$. Whereas the non-adversarial predictors aim to channel the information flow, the adversarial classifiers aim to minimize the information leakage, enforcing the information content's mutual exclusivity—the latter act as proxies for an unknown (optimal) adversarial post-classifier trained on the trained representation. At equilibrium of this minimax game, the latent space factorizes these subspaces independently.

The setup involves observational input $\boldsymbol{x} \in \mathbb{R}^k$, M target attributes $\mathbf{a} \in \mathcal{A} = A_1 \times A_2 ... A_M$, each having m_t classes $A_t = \{a_1, ..., a_{m_t}\}$, and a sensitive attribute of N classes, which is known at class level defined as $\mathcal{Y} = \{1, ..., N\}$. The goal is to learn an encoder $q(\boldsymbol{x}; \theta_E) = \boldsymbol{z}$, parameterized by θ_E producing an embedding $\boldsymbol{z} \in \mathbb{R}^h$. We want the representation to decompose into two parts $\left(\boldsymbol{z}_{tar} \in \mathbb{R}^{\hat{f}}, \boldsymbol{z}_{res} \in \mathbb{R}^g\right) = \boldsymbol{z}$. Decomposition of the representation entails two network streams. Here, $\boldsymbol{z}_{tar}$ represents the target part and residual part $\boldsymbol{z}_{res}$, respectively, which we assume w.l.o.g. to be of equal dimension. The associated process schematic is shown in Fig. 1. The encoder $\boldsymbol{z} = E(\mathbf{x}; \theta_E)$ and the decoder $\tilde{\boldsymbol{x}} = D(\mathbf{z}; \theta_D)$ are defined as deterministic functions, parameterized by θ_E and θ_D, respectively. Furthermore, $\boldsymbol{z}_{tar} = E_{tar}(\boldsymbol{x}; \theta_E)$ is the target part of the presentation. Analogously, $\boldsymbol{z}_{res} = E_{res}(\boldsymbol{x}; \theta_E)$ denotes the residual partition. The target predictor is given as $p_T(\mathbf{a}|\boldsymbol{z}_{tar}; \theta_{tar})$, the sensitive attribute predictors as $p_S(y|\boldsymbol{z}_{res}; \theta_{res})$, parameterized by θ_{tar} and θ_{res}. The associated adversarial predictors are denoted as $\tilde{p}_T(\mathbf{a}|\boldsymbol{z}_{res}; \tilde{\theta}_{tar})$ and $\tilde{p}_S(y|\boldsymbol{z}_{tar}; \tilde{\theta}_{res})$, parameterized by $\tilde{\theta}_{tar}$ and $\tilde{\theta}_{res}$. As the predictors and the adversarial predictors have competitive relationship, they are optimized differently. Whereas predictors are trained using minimization of cross-entropy, the adversarial predictors seek to maximize entropy. Consequently, we define the proposed approach as an optimization problem as a multi-player nonzero-sum game:

$$\min_{\theta_{E,T,D,S}} \max_{\theta_{\tilde{T},\tilde{S}}} \lambda \cdot \phi_{ED}(\theta_E, \theta_D) + \alpha_T \cdot \phi_T(\theta_E, \theta_{tar}) + \tag{1}$$

$$\alpha_S \cdot \phi_S(\theta_E, \theta_{res}) + \beta_{\tilde{T}} \cdot \phi_{\tilde{T}}(\theta_E, \tilde{\theta}_{tar}) + \beta_{\tilde{s}} \cdot \phi_{\tilde{S}}(\theta_E, \tilde{\theta}_{res}), \tag{2}$$

with $\phi_*(.|.)$ denoting the players, and $\lambda, \alpha_*, \beta_* \in \mathbb{R}$ weighting scalars. The hyperparameters allow for a trade-off between the utility of target classification and the latent code's privacy preservation.

3.1 Adversarial Representation Learning

In the following, we will define the optimization criterion for each player. First, we explain the predictors, followed by the reconstruction, and conclude the optimization of the adversarial classifiers, notably sanitization and herein focal entropy.

Predictors: The predictors are all modeled as conditional distributions. They are trained by:

$$\phi_T(\theta_E, \theta_{tar}) = D_{KL}(p(\mathbf{a}|\boldsymbol{x}) \| p_T(\mathbf{a}|\boldsymbol{z}_{tar}); \theta_{tar}) \tag{3}$$

$$\phi_S(\theta_E, \theta_{res}) = D_{KL}(p(y|\boldsymbol{x}) \| p_S(y|\boldsymbol{z}_{res}); \theta_{res}) \tag{4}$$

where $p(\mathbf{a}|\boldsymbol{x})$ and $p(y|\boldsymbol{x})$ denote the ground-truth labels for training input x for the target attribute and the sensitive attribute, respectively. $D_{KL}(.\|.)$ denotes the Kullback-Leibler divergence.

Reconstruction: We propose to employ a VAE for reconstruction. As such, optimization of ϕ_{ED} entails minimization of Evidence Lower Bound (ELBO). The ELBO naturally is defined as:

$$\phi_{ED}(\theta_E, \theta_D) = \mathrm{E}_{q(\boldsymbol{z}|\boldsymbol{x};\theta_E)} \left[\log p\left(\boldsymbol{x}|\boldsymbol{z}; \theta_D\right)\right] - D_{KL}(q\left(\boldsymbol{z}|\boldsymbol{x}; \theta_E\right) \| p\left(\boldsymbol{z}\right)), \tag{5}$$

which decomposes into two parts. The first term corresponds to the reconstruction likelihood measuring the error in input reconstruction. The second term corresponds to the prior constraint, where we assume isotropic Gaussian as latent prior $p\left(\boldsymbol{z}\right) = \mathcal{N}\left(0; \boldsymbol{I}\right)$, where $\boldsymbol{I}$ denotes the identity matrix. Furthermore, we assume the posterior approximates to be multivariate Gaussians. Given two separate encoding streams, one for the target and the residual part, we yield: $q\left(\boldsymbol{z}_{tar}|\boldsymbol{x}; \theta_E\right) = \mathcal{N}\left(\boldsymbol{z}_{tar}; \boldsymbol{\mu}_{tar}, \boldsymbol{\Sigma}_{tar}, \right)$ and $q\left(\boldsymbol{z}_{res}|\boldsymbol{x}; \theta_E\right) = \mathcal{N}\left(\boldsymbol{z}_{res}; \boldsymbol{\mu}_{res}, \boldsymbol{\Sigma}_{res}, \right)$, with $\boldsymbol{\mu} \in \mathbb{R}^h, \boldsymbol{\Sigma} \in \mathbb{R}^{h \times h}$.

Sanitization: In order to minimize the information leakage across representation partitions, we leverage the maximization of entropy. This enforces the representation to be maximally ignorant w.r.t. attributes in the domain confusion sense. Specifically, for the adversarial target attribute, we let

$$\phi_{\tilde{S}}(\theta_E, \tilde{\theta}_{tar}) = D_{KL}(\tilde{p}_T(\mathbf{a}|\boldsymbol{z}_{res}); \tilde{\theta}_{tar} \| U), \tag{6}$$

where U denotes the uniform distribution. Although maximization of entropy is sufficient for non-private attributes to minimize information leakage across representation partitions, we postulate that

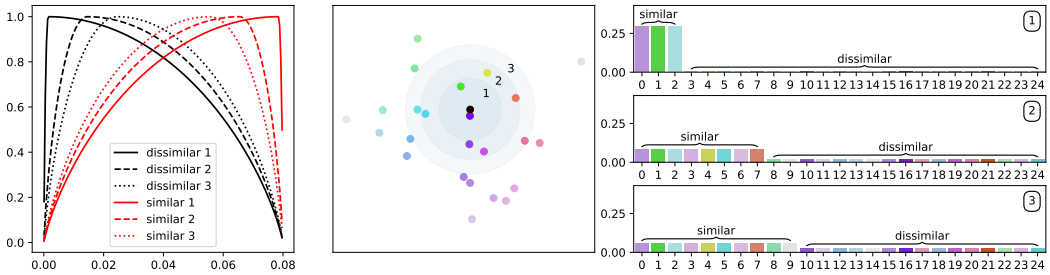


Figure 2: Illustration of focal entropy and the effect of grouping. **Center:** Visualization of a sample configuration; schematic focus regions depicted as circles ranging from narrow (1) to wide (3). **Left:** Visualization of off-center entropies (similar, dissimilar) for different focus regions scenarios. The more narrow the focus, the more weight "*similar*" samples have. Conversely, the wider focus range, the more equiprobability is approached. **Right:** Entropy visualization for focus scenarios.

proper sanitization must be conducted w.r.t to focus classes in a similarity-aware fashion. As such, we aim to sanitize the information of each observation within a focus area, i.e., nearest neighbors (NN). For each observation, the NNs share the most commonalities in features. As such, discrimination w.r.t. NNs is less likely to be trivially achievable. To this end, training of $\phi_{\tilde{T}}(\theta_E, \tilde{\theta}_{res})$ leverages a modification of entropy for deep sanitization.

3.2 Focal Entropy

First, realizing deep sanitization requires partitioning the sensitive attribute into two sets w.r.t. mutual discriminativeness: "*similar*" classes (A) "*dissimilar*" classes (B). This partitioning is input specific. Thus, let $\mathbf{s}$ be the logit scores given the observational input x, with class predictions given by any index with maximal score, i.e., $p\left(y|x;\boldsymbol{\theta}\right) = p(\mathbf{s}) \in \arg\max \mathbf{s}$. Then "*similar*" consists of the set of labels corresponding to the k largest scores, and "*dissimilar*" the complement:

$$\mathcal{Y}_{similar} = \left\{\mathbf{y} \in \mathcal{Y}^{(k)} : \forall i \in \{1, ..., k\}, s_{y_i} \geq s_{[k]}\right\}, \quad \mathcal{Y}_{dissimilar} = \mathcal{Y} \setminus \mathcal{Y}_{similar} \tag{7}$$

Here $s_{[k]}$ denotes the k-th largest element of $\mathbf{s}$, and $\mathcal{Y}^{(k)}$ denotes the set of k-tuples with k distinct elements of $\mathcal{Y}$. Grouping is conducted either according to label information provided, using a pre-trained model or "*on-the-fly*" during training. Let N_A, N_B corresponds to the number of classes in A and B, where typically $N_A \ll N_B$ holds and $N = N_A + N_B$. In case of N classes, entropy reaches maximum at uniformity, i.e., $\frac{1}{n}$. However, we would like the entropy peak shifted such that uniformity w.r.t. similar classes gets dominant. This implies reciprocal reweighting of the classes in A and B, respectively - see Fig. 2. Therefore, we define a reweighting vector $\boldsymbol{\tau} \in \mathbb{R}^N$ such that:

$$\tau_{1,...,N_A} = \frac{N_B}{N_A^2 + N_B \cdot N_A}, \tau_{N_A+1,...,N} = \frac{N_A}{N_B^2 + N_A \cdot N_B}, \text{ s.t. } \sum_i^N \tau_i = 1 \tag{8}$$

Essentially this aims at giving more weight to confusion w.r.t. members of similar classes. Analogously, members of dissimilar classes are down-weighted accordingly. As a result, the classifier is forced to be maximally ignorant w.r.t. class properties of the similar class members. That is, the feature representation produced from the encoder should not have any sensitive information in the target part. As this approach implicitly is driving sanitization by focusing on specific targets, we refer to this as "*focal entropy*". Implementation of the focal entropy criterion is essentially equivalent to maximization w.r.t. an off-centered entropy Lallich et al. (2007) in the special case of normalized uniform probability within each group. See Fig. 2 for the schematic illustration of the proposed concept. Off-centering entropy entails a transformation of the probabilities. In order to have the entropy peak at $\boldsymbol{\tau} \in \mathbb{R}^N$, each $p_i \in \mathbf{p}$ has to be remapped, where $\mathbf{p} = (p_1, ..., p_N) \in \mathbb{R}^N$ denotes the vector of probabilities. Note, in case of uniformity and N classes $\boldsymbol{\tau} = (\frac{1}{N}, ..., \frac{1}{N})$. Implementing the focusing behavior w.r.t. the similar class, π_i is defined as:

$$\pi_j = \frac{p_j}{N\tau_j} \quad \text{if } 0 \leq p_j \leq \tau_j, \quad \pi_j = \frac{N(p_j - \tau_j) + 1 - p_j}{N(1 - \tau_j)} \quad \text{if } \tau_j \leq p_j \leq 1 \tag{9}$$

CIFAR-100 Krizhevsky (2009)		
Method	Tar.	Adv.
Random Chance	1.0	0.01
Roy & Boddeti (2019)	0.71	0.16
Sadeghi et al. (2019)	0.80	0.16
Ours	**0.82**	**0.16**

CelebA Guo et al. (2016)		
Method	Tar.	Adv.
Random Chance	1.0	< 0.001
Szabo et al. (2018)	-	0.09
Harsh Jha et al. (2018)	-	0.14
Denton & Birodkar (2017)	-	0.03
Gabbay & Hoshen (2020)	-	**< 0.01**
Bouchacourt et al. (2018)	0.88	0.178
Liu et al. (2015)	0.873	-
Zhang et al. (2014)	0.854	-
Liu et al. (2018)	0.878	-
Ours	**0.90**	**< 0.01**

Table 1: Results on CelebA and CIFAR-100.

CIFAR-100 Krizhevsky (2009)		
Method	Tar.	Adv.
Random Chance	1.0	0.01
Ours (`entropy`)	0.70	0.16
Ours (`F. entropy`)	**0.82**	**0.16**

CelebA Guo et al. (2016)		
Method	Tar.	Adv.
Random Chance	1.0	< 0.001
Ours (`entropy`)	0.90	0.061
Ours (`F. entropy`)	**0.90**	**< 0.01**

Table 2: Ablation study (*Focal entropy*) on CIFAR-100 and CelebA.

CelebA Guo et al. (2016)		
Method	Tar.	Adv.
Random Chance	1.0	< 0.001
Ours (`normal cls.`)	0.90	0.007
Ours (`strong cls.`)	0.90	0.009

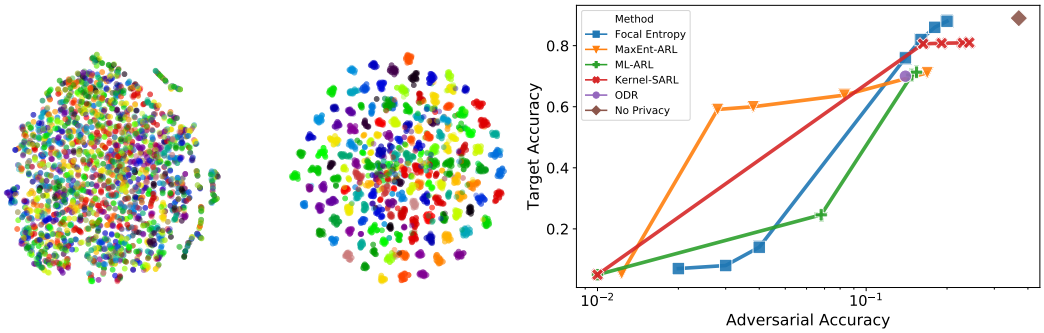
Table 3: Probing analysis on CelebA.

Technically, these π_j have to be normalized subsequently. It is only after normalization according to $\pi_j^* = \pi_j \cdot (\sum_i^N \pi_i)^{-1}$ that the properties of a proper entropy are fulfilled. It should be noted that focal entropy contrasts with conventional entropy in terms of promoting hub formation. Here a hub relates to the adversarial mapping of multiple sensitive "similar" entities, i.e., IDs for CelebA, to the same "target". Essentially, entropy drives for equiprobability of classes and thus suppresses the formation of hubs, whereas focal entropy enforces the collapse of "*similar*" sensitive entities on the same hub. Hence, entropy induces a *bijective* mapping due to its invariance to random relabeling, whereas focal entropy induces a *surjective* mapping w.r.t. hubs.

4 EXPERIMENTS

Setup: We experimentally validate the proposed method using two datasets, which exhibit different characteristics. First, the algorithm is tested on CIFAR-100 Krizhevsky (2009) dataset. It consists of 100 classes, grouped into 20 superclasses. The classes are (theoretically) entirely mutually exclusive, such that each item is associated with precisely one fine-grained category belonging to one coarse superclass. In the privacy setting, the encoder is forced to learn a representation that is superclass aware, while not revealing any information about the fine-grained classes. Second, the CelebA dataset of celebrity face images Guo et al. (2016). This dataset contains a large number of identities (people) with multiple observations of each. The "in-the-wild" nature of face images offers a richer testbed for our method as both identities and contingent factors are significant sources of variation. Furthermore, the class structure does not permit a well-defined separation between public and private spaces.

Implementation Details: We employ Stochastic Gradient Descent (SGD) with momentum 0.9 and weight-decay of $1\mathrm{e}{-4}$ and a batch size of 200, with a learning rate of 0.01. Furthermore, we employ learning rate decay at every 30th epoch by a factor of 0.1. On CelebA, to learn target and adversary classifiers smoothly, we perform pre-training without adversary objective for 100 epochs. This allows us to learn a stable representation crucial for gentle modification, i.e., channeling the information flow. Subsequently, the model is trained for another 1200 epochs, allowing for a slow "burn-in" of adversary objective such it cannot be undone. On CIFAR-100, the model is trained for 3000 epochs. As for the trade-off parameters of Eq. 2, we employ the following scheme. CIFAR: equal weights for target loss and adversary: $\alpha_S = \alpha_T = 1$, $\beta_T = \beta_S = -1$, NN size of *5*. CelebA: weighting according to number of objectives $\alpha_T = \frac{1}{40}, \alpha_S = 1.0$, $\beta_T = -\frac{1}{40}, \beta_S = -1$. For reconstructing weighting, we always assume $\lambda = 1.0$. For grouping in focal entropy, we assume the NN size of 16.



(a) t-SNE embeddings

(b) Trade-off curve

Figure 3: **Left:** t-SNE embedding of latent representation for a subset of 200 IDs. **Left t-SNE:** embedding of the target part $\boldsymbol{z}_{tar}$. **Righ t-SNE:** embedding of residual part $\boldsymbol{z}_{res}$. t-SNE is unable to reveal any sort of regular structure in $\boldsymbol{z}_{tar}$ w.r.t. private attribute. **Right:** Trade-Off curve between target accuracy and adversarial accuracy on CIFAR-100.

4.1 Privacy Sanitization Analysis

We evaluated the privacy sanitization in terms of target and adversarial accuracy on two benchmarks:

CIFAR-100: As the first testbed, we adopt the "simulated" privacy problem proposed by Roy & Boddeti (2019) designed on the CIFAR-100 dataset. We treat the *coarse* (superclass) and *fine* (class) labels as the target and sensitive attribute, respectively. The task is to learn the superclasses' features while not revealing the information about the underlying classes. Here we note that "ideally" we desire a predictor accuracy of 100%, an adversary accuracy of 1% (random chance for 100 classes). In Tab. 1, we report the accuracy achieved by the attribute predictor and adversary. From these results, we observe that with our proposed method, the representation achieves the best target accuracy while being comparable on adversary accuracy compared to the SOTA sanitization methods Roy & Boddeti (2019); Sadeghi et al. (2019). Using conventional entropy for adversary instead of our proposed *focal entropy* results in a significant performance drop (from 82% to 70% in terms of target accuracy at comparable adv. accuracy). In Fig. 3b, we report the characteristics of the proposed approach in terms of trade-off curves that portrays the correlation between privacy and target utility. We compared with the most relevant works to us: MaxEnt-ARL and ML-ARL from Roy & Boddeti (2019), Kernel-SARL Sadeghi et al. (2019), Orthogonal Disentangled Representations (ODR) from Sarhan et al. (2020), and vanilla baseline *(No Privacy)* without sanitization. As can be seen, the higher the correlation to privacy, the higher appears the loss of accuracy at a high level of sensitive accuracy. Furthermore, the proposed approach features a significantly better utility trade-off in the high target-accuracy domain. Additionally, to assess the effect of our proposed *focal entropy* in terms of the adversarial component, comparing it with conventional entropy. We report the results in Tab. 2.

CelebA: As the second testbed, we adopt the CelebA dataset, which has a richer structure to be utilized for privacy while being less structured in terms of similarity. Specifically, we treat the attribute labels as target and celebrity identity (i.e., ID) as the source of sensitive information. The task is to learn to classify the attributes while not revealing the information about the identities. We note that ideally, we desire a lower adversary accuracy (< 0.001) compared to the previous case, as the number of ID classes is an order of magnitude higher. In Tab. 1 we report the target/adversary accuracy. We observe that the representation we learn achieves a higher target accuracy and lower adversary accuracy than the strong baseline ML-VAE Bouchacourt et al. (2018). Using standard entropy instead of our proposed *focal entropy* in CelebA shows a considerable higher privacy leakage (namely, 0.061 and < 0.01) - see Tab. 2. Moreover, to analyze the sanitization of privacy in the latent representation, we visualize the t-SNE of the target and residual parts of the representation in Fig. 3a. For visualization, a subset of 200 IDs was chosen randomly from the test set. As can be seen, the private class associations appear random and cannot be recovered from the target part. This contrasts sharply with the residual part, where common IDs form clusters, giving rise to a proper margin, confirming our quantitative results in terms of target/adversary accuracy. Additionally, we

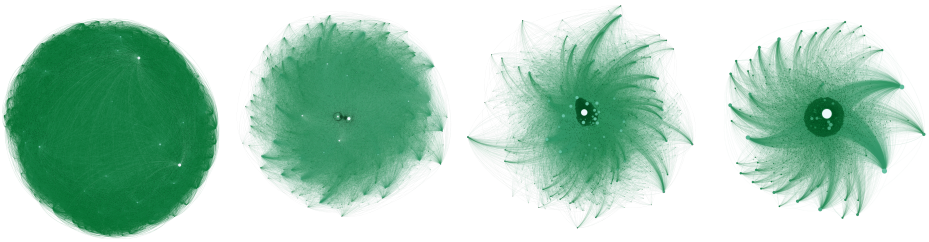


Figure 4: Visualization of adversary ID re-mapping graph on CelebA for entropy to focal entropy with different k-NNs on $\boldsymbol{z}_{tar}$. Nodes correspond to IDs, edges to adversarial re-mapping of an ID to facilitate adversary confusion. Node size/brightness scales with number of associations (the bigger/brighter, the more IDs are mapped to a specific node). From *left* to *right* increasing k for focal entropy: k =1 ($\approx$ standard entropy), 2, 16 and 64.

performed a probing experiment to assess the dependency of classifier capacity regarding the learned representation's privacy leakage potential. Specifically, we determined the adversarial accuracy on the learned representation w.r.t. to the classifier's strength. The `strong` probing classifier has approximately double the capacity of the proxy classifier that was used for training - see Tab. 3.

4.2 Hub Analysis

This section provides an analysis of how the application of focal entropy, with its integration of the notion of $k-$NN, promotes the formation of "hubs". By varying the neighborhood size k, focal entropy manifests itself between two extremes: **i)** Choosing a *small* k, focal entropy in the limit $(k = 1)$ approaches conventional entropy - no hubs are formed - remapping is a "*one-to-one*" correspondence. This can be attributed to conventional entropy being invariant to random relabeling, inducing a bijective mapping, giving rise to information preservation. This is prone to sub-optimal solutions since the forced equalization of classes by disregarding semantic similarity of classes makes the model susceptible to find shortcuts such as label swapping. In this regard, target accuracy oscillations co-occurring with degenerate ID-remappings such uniformity across all labels or temporary collapse to very few hubs were observed. **ii)** Choosing a *large* k, focal entropy promotes the formation of a single dominant hub, which is also referred to as the classical hubness problem. This phenomenon is related to the convergence of pairwise similarities between elements to a constant as the space's dimensionality increases Radovanovi263 et al. (2010) (collapsing on a single hub/trivial solution). The single hub then manifests itself as the favored result of queries Dinu et al. (2014) - giving rise to trivial solutions rather than deep sanitization. Choosing a *non-extreme* k leads to the formation of numerous equisized hubs, inducing a surjective mapping. As the formation of multi-hubs coincides with a collapse, less information is required to establish a mapping. Hence, this characteristic gives rise to information removal and is thus imperative for proper sanitization. Figure 4 depicts the graphs induced by remapping for four different neighborhood configurations.

5 Conclusion

In this paper, an adversarial representation learning method is proposed to deal with a setting where the target and sensitive attributes are related to each other to a large extent. Training the representation entails decomposition into a target and a residual part. Here, the target part is shareable without privacy infringement and facilitates applicability for a target task. In contrast, the residual part subsumes all the private non-shareable information. Our proposed adversarial learning method employs focal entropy for deep sanitization of privacy from the representation. Subsequently, our experiments confirm that our proposed method learns sanitized data representations using a manageable level of supervision. Future work will entail adaptive and "*on-the-fly*" similarity grouping during training.

REFERENCES

Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 308–318. ACM, 2016.

Frederik Armknecht, Colin Boyd, Christopher Carr, Kristian Gjøsteen, Angela Jäschke, Christian A. Reuter, and Martin Strand. A guide to fully homomorphic encryption. *IACR Cryptology ePrint Archive*, 2015:1192, 2015. URL `http://dblp.uni-trier.de/db/journals/iacr/iacr2015.html#ArmknechtBCGJRS15`.

Lars Backstrom, Cynthia Dwork, and Jon Kleinberg. Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. In *Proceedings of the 16th international conference on World Wide Web*, pp. 181–190. ACM, 2007.

Diane Bouchacourt, Ryota Tomioka, and Sebastian Nowozin. Multi-level variational autoencoder: Learning disentangled representations from grouped observations. In *Thirty-Second AAAI Conference on Artificial Intelligence*, 2018.

Jiawei Chen, Janusz Konrad, and Prakash Ishwar. Vgan-based image representation learning for privacy-preserving facial expression recognition. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pp. 1570–1579, 2018.

Elliot Creager, David Madras, Jörn-Henrik Jacobsen, Marissa A Weis, Kevin Swersky, Toniann Pitassi, and Richard Zemel. Flexibly fair representation learning by disentanglement. *arXiv preprint arXiv:1906.02589*, 2019.

Emily L Denton and vighnesh Birodkar. Unsupervised learning of disentangled representations from video. In I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett (eds.), *Advances in Neural Information Processing Systems 30*, pp. 4414–4423. Curran Associates, Inc., 2017.

Georgiana Dinu, Angeliki Lazaridou, and Marco Baroni. Improving zero-shot learning by mitigating the hubness problem, 2014.

Cynthia Dwork. Differential privacy. In *33rd International Colloquium on Automata, Languages and Programming, part II (ICALP 2006)*, volume 4052 of *Lecture Notes in Computer Science*, pp. 1–12. Springer Verlag, July 2006. ISBN 3-540-35907-9.

Cynthia Dwork, Adam Smith, Thomas Steinke, and Jonathan Ullman. Exposed! a survey of attacks on private data. *Annual Review of Statistics and Its Application*, 4:61–84, 2017.

Harrison Edwards and Amos Storkey. Censoring representations with an adversary. In *International Conference in Learning Representations (ICLR2016)*, 2 2016.

Clément Feutry, Pablo Piantanida, Yoshua Bengio, and Pierre Duhamel. Learning anonymized representations with adversarial neural networks. *arXiv preprint arXiv:1802.09386*, 2018.

Aviv Gabbay and Yedid Hoshen. Demystifying inter-class disentanglement. In *International Conference on Learning Representations (ICLR)*, 2020.

Robin C Geyer, Tassilo Klein, and Moin Nabi. Differentially private federated learning: A client level perspective. *arXiv preprint arXiv:1712.07557*, 2017.

Yandong Guo, Lei Zhang, Yuxiao Hu, Xiaodong He, and Jianfeng Gao. Ms-celeb-1m: A dataset and benchmark for large-scale face recognition. In *European Conference on Computer Vision*, pp. 87–102. Springer, 2016.

Ananya Harsh Jha, Saket Anand, Maneesh Singh, and VSR Veeravasarapu. Disentangling factors of variation with cycle-consistent variational auto-encoders. In *The European Conference on Computer Vision (ECCV)*, September 2018.

Bach Ngoc Kim, Christian Desrosiers, Jose Dolz, and Pierre-Marc Jodoin. Privacy-net: An adversarial approach for identity-obfuscated segmentation. *arXiv preprint arXiv:1909.04087*, 2019.

Diederik P Kingma and Max Welling. Auto-encoding variational bayes, 2013. cite arxiv:1312.6114.

Alex Krizhevsky. Learning multiple layers of features from tiny images. Technical report, 2009.

Stéphane Lallich, Philippe Lenca, and Benoît Vaillant. Construction of an off-centered entropy for supervised learning. In *ASMDA 2007 : XIIth International Symposium on Applied Stochastic Models and Data Analysis, May 29 - June 1, Chania, Crete, Greece*, pp. ., Crete, Greece, May 2007. C. Skiadas. URL https://hal.archives-ouvertes.fr/hal-02121319.

Ang Li, Jiayi Guo, Huanrui Yang, and Yiran Chen. Deepobfuscator: Adversarial training framework for privacy-preserving image classification. *arXiv preprint arXiv:1909.04126*, 2019.

Jiachun Liao, Chong Huang, Peter Kairouz, and Lalitha Sankar. Learning generative adversarial representations (GAP) under fairness and censoring constraints. *CoRR*, abs/1910.00411, 2019a. URL http://arxiv.org/abs/1910.00411.

Jiachun Liao, Chong Huang, Peter Kairouz, and Lalitha Sankar. Learning generative adversarial representations (gap) under fairness and censoring constraints. *arXiv preprint arXiv:1910.00411*, 2019b.

Yu Liu, Fangyin Wei, Jing Shao, Lu Sheng, Junjie Yan, and Xiaogang Wang. Exploring disentangled feature representation beyond face identification. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 2080–2089, 2018.

Ziwei Liu, Ping Luo, Xiaogang Wang, and Xiaoou Tang. Deep learning face attributes in the wild. In *Proceedings of the IEEE international conference on computer vision*, pp. 3730–3738, 2015.

Francesco Locatello, Gabriele Abbati, Thomas Rainforth, Stefan Bauer, Bernhard Schölkopf, and Olivier Bachem. On the fairness of disentangled representations. In *Advances in Neural Information Processing Systems*, pp. 14611–14624, 2019.

Christos Louizos, Kevin Swersky, Yujia Li, Max Welling, and Richard Zemel. The variational fair autoencoder. *arXiv preprint arXiv:1511.00830*, 2015.

David Madras, Elliot Creager, Toniann Pitassi, and Richard Zemel. Learning adversarially fair and transferable representations. *arXiv preprint arXiv:1802.06309*, 2018.

H Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, et al. Communication-efficient learning of deep networks from decentralized data. *arXiv preprint arXiv:1602.05629*, 2016.

Arvind Narayanan and Vitaly Shmatikov. How to break anonymity of the netflix prize dataset. *arXiv preprint cs/0610105*, 2006.

Seyed Ali Osia, Ali Shahin Shamsabadi, Ali Taheri, Kleomenis Katevas, Hamid R Rabiee, Nicholas D Lane, and Hamed Haddadi. Privacy-preserving deep inference for rich user data on the cloud. *arXiv preprint arXiv:1710.01727*, 2017.

Seyed Ali Osia, Ali Taheri, Ali Shahin Shamsabadi, Minos Katevas, Hamed Haddadi, and Hamid RR Rabiee. Deep private-feature extraction. *IEEE Transactions on Knowledge and Data Engineering*, 2018.

Francesco Pittaluga, Sanjeev Koppal, and Ayan Chakrabarti. Learning privacy preserving encodings through adversarial training. In *2019 IEEE Winter Conference on Applications of Computer Vision (WACV)*, pp. 791–799. IEEE, 2019.

Novi Quadrianto, Viktoriia Sharmanska, and Oliver Thomas. Discovering fair representations in the data domain. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 8227–8236, 2019.

Miloš Radovanovi263, Alexandros Nanopoulos, and Mirjana Ivanovi263. Hubs in space: Popular nearest neighbors in high-dimensional data. *Journal of Machine Learning Research*, 11(86): 2487–2531, 2010. URL http://jmlr.org/papers/v11/radovanovic10a.html.

Proteek Chandan Roy and Vishnu Naresh Boddeti. Mitigating information leakage in image representations: A maximum entropy approach. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2019.

Michael S Ryoo, Brandon Rothrock, Charles Fleming, and Hyun Jong Yang. Privacy-preserving human activity recognition from extreme low resolution. In *Thirty-First AAAI Conference on Artificial Intelligence*, 2017.

Bashir Sadeghi, Runyi Yu, and Vishnu Boddeti. On the global optima of kernelized adversarial representation learning. In *The IEEE International Conference on Computer Vision (ICCV)*, October 2019.

Ahmed Salem, Apratim Bhattacharya, Michael Backes, Mario Fritz, and Yang Zhang. Updates-leak: Data set inference and reconstruction attacks in online learning. *arXiv preprint arXiv:1904.01067*, 2019.

Mhd Hasan Sarhan, Nassir Navab, Abouzar Eslami, and Shadi Albarqouni. Fairness by learning orthogonal disentangled representations. *European Conference on Computer Vision (ECCV)*, 2020.

Brij Mohan Lal Srivastava, Aurélien Bellet, Marc Tommasi, and Emmanuel Vincent. Privacy-preserving adversarial representation learning in asr: Reality or illusion? *Proc. Interspeech 2019*, pp. 3700–3704, 2019.

Attila Szabo, Qiyang Hu, Tiziano Portenier, Matthias Zwicker, and Paolo Favaro. Challenges in disentangling independent factors of variation, 2018.

Qizhe Xie, Zihang Dai, Yulun Du, Eduard Hovy, and Graham Neubig. Controllable invariance through adversarial feature learning. In *Advances in Neural Information Processing Systems*, pp. 585–596, 2017.

Tsung-Yen Yang, Christopher Brinton, Prateek Mittal, Mung Chiang, and Andrew Lan. Learning informative and private representations via generative adversarial networks. In *2018 IEEE International Conference on Big Data (Big Data)*, pp. 1534–1543. IEEE, 2018.

Ning Zhang, Manohar Paluri, Marc'Aurelio Ranzato, Trevor Darrell, and Lubomir Bourdev. Panda: Pose aligned networks for deep attribute modeling. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 1637–1644, 2014.