ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 2 - 2026

Legal Challenges and Countermeasures for the Protection of Individual Privacy Rights in the Internet Era

Kunchi Wang[1], *BaominWang*[1] *and Xingyu Su*[1,*]

[1] Law School, Xi'an JiaotongUniversity, Xi'an710049, Shanxi, China
[2] Law And Politics School, Lingnan Normal University, Zhanjiang 524000, Guangdong, China

SUMMARY: *In the digital networking age, safeguarding individual privacy encounters numerous legal hurdles, including data breaches and improper utilization. Differential privacy algorithms, serving as the central privacy - safeguarding technology, achieve the goal of making query outcomes and adjacent datasets indistinguishable from one another. This is accomplished by introducing random noise into the data, thereby averting the disclosure of personal information.This paper, building upon the differential privacy algorithm, puts forward a differential privacy protection approach (DeepLIFT) founded on an adaptive Gaussian mechanism. This method first computes the correlation between the input and output. It then guarantees that the differential privacy criteria are satisfied. Subsequently, it employs the feature perturbation technique to introduce noise into the correlation. After that, it constructs subsequent hidden layers to preserve data usability.The findings indicate that the DeepLIFT algorithm can efficiently quantify the contribution of features in privacy protection applications. Moreover, it offers data - based support for assessing and optimizing privacy measures. However, its effectiveness depends on the specific protection measures and model structure, so in practical applications, it is necessary to combine multiple methods to ensure comprehensive privacy protection. To summarize, this paper suggests that the problem of preventing the leakage of personal privacy information can be solved through the joint participation of individuals, enterprises and governments.*

KEYWORDS: *Differential Privacy; DeepLIFT; Data Leakage; Privacy Protection; Challenges and Countermeasures*

1 Introduction

In the current background of the frequent occurrence of network privacy infringement problems worldwide, The safeguarding of privacy within the network information data context across different nations is also an extremely grave circumstance, and the serious consequences caused by the privacy leakage of countries and individuals are alarming [1-4]. According to the survey, more than 80% of Internet users around the world have suffered bad consequences due to privacy leakage, and in the black industry chain, there are more than 1.5 million employees selling other people's private information for profit, and in two years' time a total of 6.5 billion times of privacy information data was leaked, resulting in economic losses of up to 91.4 billion yuan [5-8]. The persistent issue of personal privacy violation in the online environment has not only caused significant distress and anxiety to the public, seriously affecting their daily working

*suxingyusylvin@126.com
https://doi.org/10.65102/is2026606
Published: 30 April, 2026

life, but also brought obstacles to the economic and cultural construction of the country, affecting social stability and even triggering turmoil [9-12]. Therefore, The matter of safeguarding individual privacy within the digital network setting is of great immediacy.

Since the advent of the Internet, safeguarding personal privacy within the online realm has emerged as a prominent subject in contemporary society. The academic sphere and the judicial field have consistently engaged in discussions regarding relevant matters. In today's Internet environment, new types of privacy infringement cases are increasingly frequent, This refers to the swift advancement and extensive application of large - scale data technology, the digitization of citizens' information and privacy data is greatly deepened and triggered by the direct problem, which is manifested in the form of the traditional privacy conflict is getting more and more intense.Moreover, the semantic range and implication of the privacy right have undergone changes as well, along with the safeguarding of the privacy right in the new context of the requirements of the new context is also more and more urgent [13-17]. Although each country has issued some relevant laws and regulations and other normative documents, which have laid the foundation for rectifying the online data environment and shaping a harmonious online order [18]. However, the existing privacy legislation, judicial protection, administrative supervision and other measures are still unable to realize the standardization and effective management of the network environment.

Existing literature has also been targeted to explore the issues of relevant privacy protection laws. For example, Yang and Xu [19] discovered that the Cybersecurity Law of the People's Republic of China in China, does not have legal provisions for residential data collected by smart city-related facilities, as well as practical residential data privacy protection laws. Zhu et al. [20] investigated that consumer privacy protection policies in Chinese e-commerce websites have not eliminated consumer privacy concerns, and that the acceptance and influence of the policies are limited, and the current Chinese legislation is difficult to comprehensively cover e-commerce consumer privacy protection. Creemers [21] conducted an analysis of China's legislative procedures regarding the safeguarding of personal data privacy in the network. This analysis spanned from the 2016 Cybersecurity Law of the People's Republic of China to the 2021 Personal Information Protection Law (PIPL) and Data Security Law (DSL). The PIPL serves to connect the technology industry and consumers. Meanwhile, the DSL puts forward data protection measures at the levels of national security and public interest. Lin [22] talks about how the prima facie rule or the principle of inversion of causation in China's personal privacy breach infringement determination will still have concerns such as the lack of legality and the confusion between behavior and damage, and that it is possible to combine the principles of liability, security, and infringement of the PIPL and the DSL to determine the causality of the infringement. principle to determine the causality of the infringement, which will help in the final determination. Feng [23] puts forward four suggestions Regarding the protection of personal data in China law, namely, individuals to strengthen privacy protection, careful reference to the legislative experience of Western countries, practical legislation based on China's national conditions, and the implementation of more substantive protection regulations. Guo et al [24] highlight the safeguarding of privacy via the presentation of personal information within China's civil law. Nevertheless, the conversion of privacy content into personal information impedes the efficacy of this kind of protection.

As a result, they propose that privacy protection and personal data protection can shift from a sole civil law approach to a dual - protection framework of Chinese civil law combined with criminal law.Moreover, Sudarwanto and Kharisma [25] carried out a comparison of the personal data protection laws in Hong Kong (China), Indonesia, and Malaysia. They discovered that Indonesia has not yet set up a dedicated personal data protection law and a personal data protection commission. Additionally, there has been no standardized regulation for criminal

adjudications of personal data breaches and civil damages. Syahwami and Hamirul [26] investigated the Indonesian Constitution's privacy protection for internet users, and due to the vagueness, outdated and obsolete nature, and insufficient provisions on the uniqueness of digital technology in the constitutional legislation on internet users' digital privacy, internet users did not believe that the law could effectively protect their privacy. Sasea and Sakmaf [27] found that both digital banking services and legal status in Indonesia are regulated in the relevant banking laws, and while there are consumer protection principles for consumers, there is a dearth of specific legal stipulations regarding the safeguarding of personal data. Ayunda [28] posits that in the realm of e - commerce personal data protection in Indonesia, expediting the enactment of the Personal Data Protection Bill can effectively safeguard the privacy of personal data and offer security for e - commerce endeavors.

While Toyi and Hamidun [29] reported that the law in the digital era suffers from the contradiction between technological iteration and legislative lag, the contradiction between decentralized authority and individual rights, and the complex jurisdictional issues of international cyberlaw, and suggested the construction of a nationwide digital legal ecosystem to achieve the functions of reforming laws, regulatory harmonization, and personal data protection. Xie [30] further uncovers the legal conundrum in the cross - border transfer of personal data. Firstly, there is a dearth of global governance and disparities in legislation. Secondly, the lack of clarity regarding the rules of extraterritorial application in the legislation gives rise to jurisdictional issues. To address these problems, it is necessary for international organizations, governments, and enterprises to collaborate in improving the legislation. Lundstedt [31] indicates that the General Data Protection Regulation implemented by the EU has set up jurisdictional regulations in a cross - border scenario. Under this regulation, the data owner has the right to initiate a lawsuit either in the country of their habitual residence or in the country where the infringer and the infringing data processor are located.Politou et al [32] discuss the contentious aspects of the right to withdraw consent and the right to be forgotten within the General Data Protection Regulation, specifically in relation to the methods of personal data processing, emphasizing that this controversy requires the development of clear, cross-platform guidelines and norms that encompass all the listings and complexities in the regulation.

In this research paper, to investigate the issue of personal privacy information disclosure, a differential privacy algorithm is presented. This algorithm guarantees that individual data remains indistinguishable in statistical disclosures by incorporating a regulated noise mechanism into the query data outcomes. To safeguard differential privacy while also achieving high classification precision, this paper puts forward a differential privacy protection approach based on an adaptive Gaussian mechanism.First, the algorithm computes the input - output correlation that adheres to differential privacy. Subsequently, it utilizes correlation feature perturbation to introduce adaptive noise for highly sensitive dimensions. To enhance the practicality of the model, a local response regularization layer (LRN) is incorporated during the construction of the subsequent hidden layer. This helps to strengthen the privacy - preserving capabilities of the model under the Gaussian mechanism. Through a series of experiments, an in - depth analysis is conducted on how factors like the privacy budget and query ratio influence the algorithm's performance. Subsequently, case studies are employed to examine the effectiveness of the algorithm in safeguarding personal privacy. Finally, the root causes of personal information leakage are identified and summarized, and corresponding countermeasures are put forward.

2 Differential Privacy Protection Model for Individual Privacy in the Internet Age

2.1 Differential Privacy Algorithm

2.1.1 Differential Privacy Algorithm Definition

Differential privacy protects not the security of the entire dataset, but the security of each individual piece of data in the dataset, so that the impact of each piece of data on the overall dataset is limited, and there will not be a situation where the query result is significantly changed when one piece of data is added or subtracted. Therefore, the attacker cannot get the personal privacy of a specific user from the query result, i.e., the attacker cannot speculate which piece of data belongs to which dataset based on the information obtained.

Definition 1 (Neighboring dataset): If any two datasets D_1, D_2 are identical except for one record, then D_1, D_2 are neighboring datasets, also called brother datasets.

Neighboring datasets D_1, D_2 are shown in Fig. 1, D_1, D_2 are identical except for a record in region d, D_1 can get D_2 by adding a record in region d, or D_2 can get D_1 by deleting a record in region d, so D_1, D_2 are neighboring datasets.

Region	Number of People
a	5
b	16
c	12

Region	Number of People
a	5
b	16
c	12
d	1

Figure 1: Adjacent data sets D_1 and D_2

Definition 2 (ε-differential privacy): if any output $O \subseteq \text{Range}(\mathcal{K})$ of a randomized algorithm $\mathcal{K}$ on any two neighboring datasets D_1, D_2 satisfies the following equation:

$$\frac{\Pr\left[\mathcal{K}(D_1) \in O\right]}{\Pr\left[\mathcal{K}(D_2) \in O\right]} \le e^{\varepsilon} \tag{1}$$

Then the algorithm $\mathcal{K}$ satisfies ε-differential privacy.

In this definition, the privacy budget ε determines the degree of privacy protection of the differential privacy algorithm $\mathcal{K}$. The smaller ε indicates that the closer the algorithm's outputs are on neighboring datasets, the more impossible it is for a privacy attacker to determine the differences between neighboring datasets from the outputs, thus making the algorithm able to provide a higher strength of privacy protection, and vice versa.

Definition 3 (Global Sensitivity): for any query function $f : X \to \mathbb{R}^d$, its global sensitivity Δf is defined as:

$$\Delta f = \max_{D_1, D_2 \in X} \left\| f(D_1) - f(D_2) \right\|_1 \tag{2}$$

where the datasets D_1, D_2 are a pair of neighboring datasets, $\left\| f(D_1) - f(D_2) \right\|_1$ denotes the first-order paradigm distance of the function's query result on D_1, D_2.

The global sensitivity Δf is just one of the properties of the function f, independent of the size of the dataset, which mainly indicates the maximum change in the result of the function caused by the addition (or deletion) of an element in the dataset. The smaller Δf is, the less amount of noise needs to be introduced to mask the effect of the change of an element in the dataset on the output result of the function.

2.1.2 Noise mechanisms for differential privacy

(1) Laplace mechanism

Two frequently employed noise mechanisms in differential privacy are the Laplace mechanism and the Gaussian mechanism. The Laplace mechanism incorporates Laplace noise into the output, whereas the Gaussian mechanism adds Gaussian noise to the output. The selection of the mechanism hinges on the particular privacy and utility requirements of the application. The quantity of noise added is directly associated with the sensitivity of the computational function and the privacy parameter ε. Smaller direct values of ε offer more robust privacy assurances. The Laplace mechanism utilizes the L1 function sensitivity.

Definition 4 Laplace distribution: a Laplace distribution of scale b (centered at 0) is a distribution with a probability density function:

$$Lap\left(x \middle| (u,b)\right) = \frac{1}{2b} \exp\left(-\frac{|x-u|}{b} \right) \tag{3}$$

The variance of this distribution is $\sigma^2 = 2b^2$. In this paper, we will sometimes use $Lap(b)$ to denote the Laplace distribution with scale b, and sometimes $Lap(b)$ to denote the random variable $X \sim Lap(b)$. where μ is the expectation of the variable x and b is the scale parameter of the variable x. The Laplace distribution can be viewed as a symmetric form of the exponential distribution when $\mu = 0$, and the Laplace mechanism will simply compute f and perturb each coordinate with noise extracted from the Laplace distribution.

Definition 5 Laplace mechanism: for any function f the following definition is satisfied:

$$\mathcal{M}_L(x, f(\cdot), \varepsilon) = f(x) + (Y_1, \ldots, Y_k) \tag{4}$$

where Y_i is the i random variable extracted from Lap as $(\Delta f / \varepsilon)$. For differential privacy, the Laplace noise is computed by $Lap(\Delta f / \varepsilon)$, where: ε is the differential privacy preserving parameter, Δf is the global sensitivity, and the added noise is inversely proportional to ε and proportional to Δf.

(2) Functional sensitivity

As mentioned in the discussion of the Laplace mechanism in this paper, the quantity of noise necessary to guarantee differential privacy for a specific query is contingent upon the query's sensitivity. The sensitivity of a function indicates the extent of alteration in the function's output when the input undergoes a change.

Definition 6 Laplace mechanism function:

$$F(x) = f(x) + Lap\left(\frac{s}{\varepsilon}\right) \tag{5}$$

where $f(x)$ is a deterministic function that can be used in queries, ε is the privacy parameter, and F is the sensitivity of s. For a function $f : \mathcal{D} \to R$ mapping the dataset $(\mathcal{D})$ to the real numbers, the L1 global sensitivity function is defined as follows:

$$\Delta_2(f) = \max_{\substack{x,y \in N|X| \\ \|x-y\|_1 = 1}} \left\| f(x) - f(y) \right\|_1 \tag{6}$$

Here, $d(x, y)$ denotes the distance between two datasets x and y, which are considered to be nearest neighbors if their distance is 1 or less.

L2 global sensitivity function:

$$\Delta_2(f) = \max_{\substack{x,y \in N|X| \\ \|x-y\|_1 = 1}} \left\| f(x) - f(y) \right\|_2 \tag{7}$$

Global sensitivity is defined as the difference between $f(x)$ and $f(y)$ not exceeding $\Delta 2(f)$ for any two neighboring datasets. It is independent of the actual dataset being queried (for any neighboring x and y).

(3) Gaussian Mechanism

The Gaussian mechanism serves as an alternative to the Laplace mechanism. Unlike the Laplace mechanism, which employs Laplace noise, the Gaussian mechanism utilizes Gaussian noise.

Definition 7 According to the Gaussian mechanism, for a function $F(x)$ that returns a number, the following definition satisfies (ε, δ) differential privacy:

$$F(x) = f(x) + \mathcal{N}(\sigma^2) \tag{8}$$

where σ^2 takes the following values:

$$\sigma^2 = \frac{2s^2 \log(1.25/\delta)}{\varepsilon^2} \tag{9}$$

For $\delta^2 > 2\ln(1.25/\delta)$ and $c\Delta^2(f)/\varepsilon$, the Gaussian mechanism with $\varepsilon \in (0,1)$ and parameter σ is satisfied by the (ε, δ) -differential private, where s is the sensitivity of f and the output function samples $\mathcal{N}(\sigma^2)$ come from a Gaussian (normal) distribution centered at 0.

(5) Relaxed Difference Privacy

Relaxation differential privacy is a variation of differential privacy. It modifies the definition of differential privacy by loosening its constraints. Instead of using the typical noise range, it employs a smaller one. This adjustment is made to enhance the accuracy of queries. When compared to conventional differential privacy, it is more flexible in terms of privacy protection and also better in terms of providing good query accuracy. However, it is slightly

less secure and privacy-protective relative to Conventional differential privacy demands a case - by - case assessment and balancing.

Definition 8 Relaxed differential privacy, also known as (ε,δ) -differential privacy, has the following definition:

$$\Pr[F(x)=S]\le e^{\varepsilon}\Pr\left[F(x')=s\right]+\delta \tag{10}$$

A new privacy parameter δ is added to denote the defined "probability of failure". With the probability $1-\delta$, this research paper will receive the same assurance as that of pure differential privacy.

$$\frac{\Pr[F(x)=S]}{\Pr\left[F(x')=s\right]}\le e^{\varepsilon} \tag{11}$$

With the addition of the new privacy parameter δ, the guarantee of differential privacy becomes (ε,δ) -differential privacy, where δ denotes the probability of failure and ε denotes the strength of privacy protection. Compared to pure differential privacy, (ε,δ) -differential privacy provides the same privacy protection guarantee with probability $1-\delta$. Typically $\delta\le\ln 2$ or less is required to ensure that the probability of a privacy breach is very small. In practice, the mechanism of (ε,δ) -differential privacy usually does not fail as catastrophically as the definition allows, and thus can provide high-quality data analytics results while guaranteeing privacy.

There are two approaches to combining mechanisms in differential privacy: sequential and parallel combinations. The Advanced Combination Theorem is commonly used to denote instances of $k-fold$ adaptive combination, where k is the number of mechanisms. A $k-fold$ adaptive combination is composed of a series of mechanisms m_i, each of which m_i can choose its own input based on the outputs of the previous mechanisms. If each mechanism satisfies (ε,δ) -differential privacy, then the entire k -fold adaptive combination will satisfy $(\varepsilon',k\delta+\delta')$ -differential privacy.

$$\varepsilon'=2\varepsilon\sqrt{2k\log(1/\delta')} \tag{12}$$

The amalgamation of these mechanisms has the potential to diminish the privacy expense and yield superior data - analysis outcomes.In experiments, sophisticated combinations of loosened differential privacy are typically employed to achieve privacy safeguarding for Gaussian mechanisms.

2.2 Differential privacy preserving method based on adaptive Gaussian mechanism

To address the shortcomings of directly applying existing methods in deep domain adaptive scenarios with the help of publicly available datasets, this paper proposes a privacy-preserving deep learning method based on adaptive Gaussian mechanism (DeepLIFT). The method has a low model complexity, the overall privacy budget does not increase with the cumulative number of training rounds, and the privacy budget is simple to compute. The method consists of the following three main parts:

(1) The correlation matrix between input features and output parameters is obtained by

DeepLIFT computation, and it is used as the main basis for noise addition in the input layer.

(2) Using the DeepLIFT method that satisfies the Gaussian distribution of noise perturbation correlation calculation process exposed to the target domain data, making the correlation calculation process satisfy differential privacy.

(3) Drawing upon the correlation matrix established between the input variables and the output variables, the input layer perturbation based on the adaptive Gaussian mechanism is carried out, and the subsequent hidden layer is constructed on this basis.

2.2.1 Input-output correlation computation satisfying differential privacy preservation

DeepLIFT obtains more accurate correlation values between the input and output in deep neural networks by combining the gradient values of backpropagation with the importance of the features themselves. DeepLIFT begins by establishing the disparity between the input and output of the target and those of the "reference" - this disparity is referred to as the reference difference. With t denoting the target output neuron, with $x_1, x_2, ..., x_n$ for neurons in the middle layer of the neural network, and t^0 for the “reference” output, with $\Delta t = t - t^0$. At this point, Δt is the reference variance, which is the sum of the contributions of individual neurons, i.e.:

$$\sum_{i=1}^{n} C_{\Delta x_i} \Delta t = \Delta t \tag{13}$$

where the selection of the reference output t^0 can be chosen based on domain-specific knowledge, e.g., an all-black image can be used as a reference in a classification task targeting the MNIST dataset; a distorted rendition of the initial image can serve as a point of reference in a categorization task focused on the CIFAR dataset. By defining the reference output, DeepLIFT can make $C_{\Delta x_i \Delta t}$ can also be a non-zero value when $\frac{\partial t}{\partial x_i}$ is zero. So by the above method, DeepLIFT solves the problem of inability to simulate gradient saturation in existing work. The use of reference differences allows neurons to propagate important signals even when the gradient is zero.

For a neuron x with a reference difference of Δx and a target neuron with a reference difference of Δt, the contribution of the neuron x to the target neuron t is then defined as the multiplier $m_{\Delta x \Delta t}$, i.e.:

$$m_{\Delta x \Delta t} = \frac{C_{\Delta x \Delta t}}{\Delta x} \tag{14}$$

Denote the input layer neurons as $x_1, x_2, ..., x_n$, hidden layer neurons denoted as $y_1, y_2, ..., y_n$, and the target output denoted as t. Given the contribution $m_{\Delta x_i \Delta y_t}$ of neuron x to neuron y and the contribution $m_{\Delta y_t \Delta t}$ of neuron y to the target output t, the contribution $m_{\Delta x_i \Delta t}$ of neuron x to the target output t can be found by the chain rule, calculated as:

$$m_{\Delta x_i \Delta t} = \sum_j m_{\Delta x_i \Delta y_t} m_{\Delta y_t \Delta t} \tag{15}$$

Combining the defined reference differences and the chain rule for multipliers, the contribution of any neuron relative to the target output can be computed given each neuron and

its subsequent multipliers. The rules for assigning contribution scores are as follows:

(1) Let y be a linear function $y = b + \sum_i \omega_i x_i$ of the input feature x_i, which yields $\Delta y = \sum_i \omega_i x_i$. Define the equations for the positive and negative contributions to Δy as:

$$\Delta y^+ = \sum\nolimits_i 1\{\omega_i \Delta x_i > 0\} \omega_i \left(\Delta x_i^+ + \Delta x_i^-\right) \tag{16}$$

$$\Delta y^- = \sum\nolimits_i 1\{\omega_i \Delta x_i < 0\} \omega_i \left(\Delta x_i^+ + \Delta x_i^-\right) \tag{17}$$

(2) The contribution options can be obtained as follows:

$$C_{\Delta x_i^+ \Delta y^+} = 1\{\omega_i \Delta x_i > 0\} \omega_i \Delta x_i^+ \tag{18}$$

$$C_{\Delta x_i^- \Delta y^+} = 1\{\omega_i \Delta x_i > 0\} \omega_i \Delta x_i^- \tag{19}$$

$$C_{\Delta x_i^+ \Delta y^-} = 1\{\omega_i \Delta x_i < 0\} \omega_i \Delta x_i^+ \tag{20}$$

$$C_{\Delta x_i^+ \Delta y^-} = 1\{\omega_i \Delta x_i < 0\} \omega_i \Delta x_i^+ \tag{21}$$

(3) can be obtained from the previous definition of multiplier:

$$m_{\Delta x_i^+ \Delta y^+} = m_{\Delta x_i^- \Delta y^+} = 1\{\omega_i \Delta x_i > 0\} \omega_i \tag{22}$$

$$m_{\Delta x_i^+ \Delta y^-} = m_{\Delta x_i^- \Delta y^-} = 1\{\omega_i \Delta x_i < 0\} \omega_i \tag{23}$$

Since in the process of calculating the correlation between the input features and the output, the algorithm comes into contact with the target domain data that contains the user's personal privacy in the input data. In this paper, the Gaussian mechanism is utilized to perturb the computed input-output correlation results, and the perturbation process is as follows:

(1) The average feature importance of all j input features obtained is denoted as $R_j(D)$:

$$R_j(D) = \frac{1}{|D|} \sum_{x_i \in D} R_{x_{ij}}(x_i) \tag{24}$$

(2) The sensitivity of R_j can be calculated:

$$\Delta_R = \max_{D_1, D_2} \left\| R(D_1) - R(D_2) \right\|_2 = \frac{2\sqrt{d}}{D} \tag{25}$$

where d denotes the dimension of the feature and D denotes the amount of data contained in the dataset.

(3) In this paper, the correlation calculation process is made to satisfy differential privacy by adding a Gaussian distribution noise to the input-output correlation result, and the result after perturbing the average correlation of each feature j is denoted as $\bar{R}_j(D)$. After bringing in

the results of the sensitivity calculation, $\bar{R}_j(D)$ is:

$$\bar{R}_j(D) = \frac{1}{|D|}\sum_{x_i \in D} R_{x_{ij}}(x_i) + \mathcal{N}\left(0, \frac{4d^2 \log\left(\frac{1.25}{\delta_1}\right)}{\varepsilon_1^2 D^2}\right) \tag{26}$$

The privacy budget consumed in this step is $(\varepsilon_1, \delta_1)$, the average feature importance after perturbation:

$$\bar{R}(D) = \{\bar{R}_j\}_{j \in [1,d]} \tag{27}$$

2.2.2 Relevance feature perturbation methods

In general, the affine transformation of a neuron $h \in h_0$ can be expressed as:

$$h_{x_i}(W) = b + x_i W^T \tag{28}$$

where b is the static bias and W is the weight parameter of the neuron. For a given training batch L, h can be written as:

$$h_L(W) = \sum_{x_i \in L}\left(b + x_i W^T\right) \tag{29}$$

In order for the input layer h_0 to satisfy differential privacy, for each neuron expression h_L in the input layer h_0, the static bias b and the input features x_i need to be noisily perturbed during the computation. In order to realize adaptive noise addition, the privacy budget ratio β_j needs to be defined first:

$$\beta_j = \frac{d \times \left|\bar{R}_j\right|}{\sum_{j=1}^{d}\left|\bar{R}_j\right|} \tag{30}$$

β_j denotes the ratio of the privacy budget to be allocated for the corresponding feature to the total privacy budget. Based on β_j the privacy budget ε_j allocated to each of the corresponding j input features can be calculated:

$$\varepsilon_j = \beta_j \times \varepsilon_2 \tag{31}$$

The sensitivity $\Delta_{h_0} = \sum_{h \in h_0}\sqrt{d}$ can be computed according to the realization mechanism. Each feature x_{ij} of each hidden neuron h in the first layer needs to be perturbed, and the perturbation result is:

$$\bar{x}_i = x_i + \frac{1}{|L|}\mathcal{N}\left(0, \frac{\Delta_{h_0}^2 \log\left(\frac{1.25\beta_j}{\delta_2}\right)}{\varepsilon_j^2}\right) \tag{32}$$

The disturbed input features are denoted as $\bar{x}_t$. For a given training batch L, an affine transform layer $\bar{h}_{0L}$ satisfying differential privacy preservation can be constructed, which includes the interfered neurons $\bar{h}_L(W)$:

$$\bar{h}_{0L}(W_0) = \left\{\bar{h}_L(W)\right\}_{h \in h_0} \tag{33}$$

Among them:

$$\bar{h}_L(W) = \sum_{x_i \in L}\left(\bar{x}_i W^T + \bar{b}\right) \tag{34}$$

Similarly, the static bias b can be perturbed based on the Gaussian mechanism, and the perturbation results in:

$$\bar{b} = b + \frac{1}{|L|}\mathcal{N}\left(0, \frac{\Delta_{h_0}^2 \log\left(\frac{1.25}{\delta_2}\right)}{\varepsilon_2^2}\right) \tag{35}$$

2.2.3 Subsequent hidden layer construction

In this paper, a local response regularization layer (LRN) is applied to each hidden layer after an activation function such as ReLUs is used to restrict the output result value of the activation function to be between $[0,1]$.

For fully connected layers, given an input x_i, each post-interference neuron $\bar{h}_{x_i}(W)$ can be regularized to $\bar{h}_{x_i}$:

$$\bar{\bar{h}}_{x_i} \leftarrow \frac{\bar{h}_{x_i}(w) - \chi}{\varphi - \chi} \tag{36}$$

where φ and χ represent the maximum and minimum values in $\bar{h}_{x_i}$, respectively.

For the interfered neuron $\bar{h}_{ij}^k$ in the convolutional layer located at the (i, j) position of the k th feature map can be regularized to $\bar{h}_{ij}^k$ based on the regularization method:

$$\bar{h}_{ij}^{k} \leftarrow \frac{\bar{h}_{ij}^{k}}{\max\left(\bar{h}_{ij}^{k}, \left(q+\alpha\sum_{m=\max\left(0,k-\frac{l}{2}\right)}^{\min\left(N-1,k+\frac{l}{2}\right)}\left(\bar{h}_{ij}^{m}\right)^{2}\right)^{\beta}\right)} \tag{37}$$

where q,α,a,l are hyperparameters and N is the total number of feature maps. The values of the hyperparameters are set to $q=2,l=5,\alpha=10^{-4},\beta=0.75$.

2.3 Effect of different parameters on DeepLIFT performance

This section compares the performance of different methods under different parameters. They are query ratio, privacy budget, number of attributes and attribute fetch space size.

In this paper, ANoise algorithm and GNoise algorithm are used as comparison algorithms, and the effectiveness of the application of this paper's algorithm DeepLIFT with the 2 comparison algorithms is tested in the trajectory sampling dataset Geolife.

2.3.1 Impact of the privacy budget

The impact of varying the privacy budget on the mean absolute error of each approach is depicted in Figure 2. Evidently, the DeepLIFT approach holds a notable edge over the comparison approaches.Moreover, in comparison with other methods, the average absolute error of the DeepLIFT method is more significantly influenced by alterations in the privacy budget. This phenomenon can be explained as follows: Since both DeepLIFT methods mitigate the problem of noise aggregation as well as dimensionality catastrophe, the privacy budget becomes the only parameter that affects the utility of both. In contrast, the utility of the other methods is affected by a variety of factors, so that only increasing the privacy budget does not provide a significant improvement in their effectiveness.

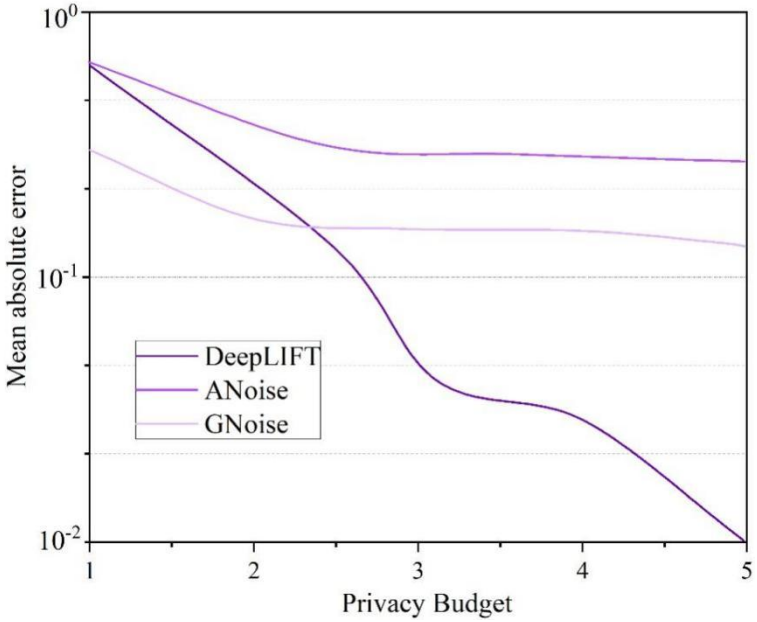

Figure 2: Impact of privacy budget changes on average absolute error

2.3.2 Effect of the number of attributes

The effect of variation in the number of attributes on the absolute mean error of each method is shown in Figure 3. It can be observed that the DeepLIFT method consistently outperforms the other methods. By and large, the average absolute error of all methods increases with the number of attributes, which is due to the fact that when the number of marginal distributions or pre-relaxations to be collected increases, the localized differential privacy noise contained in the range query results increases consequently. In addition, several outliers can be found in the experimental results the average relative error of the DeepLIFT method when the number of attributes is equal to 50 is smaller than the average relative error when the number of attributes is equal to 40. This is caused by the change in the size of the base set. In detail, when the number of attributes increases from 40 to 50, the optimal base set size determined according to the guideline rule changes, i.e., the base set size corresponding to the user record when it has 50 attributes is instead smaller. The smaller set size results in a change in the prefixes and number of prefixes to be collected, and the localized differential privacy noise introduced is reduced.

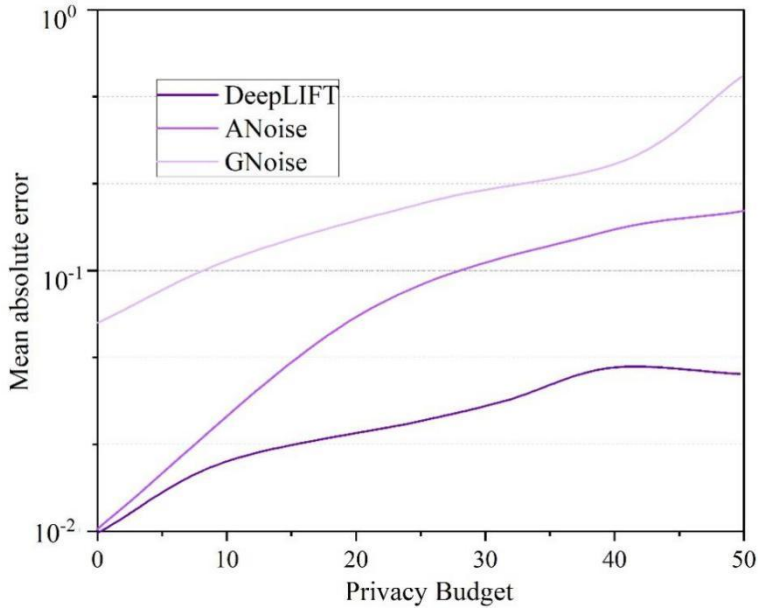

Figure 3: The effect of attribute quantity change on absolute mean error

2.3.3 Effect of query ratio

The impact of the query proportion on the performance of each method is depicted in Figure 4.It can be observed that as the query proportion grows, the average absolute error of all methods increases. It is worth noting that the average absolute error of DeepLIFT methods decreases as the query proportion grows, this is because the number of records involved in a single range query increases as the query proportion grows, whereas the error of the range query result in DeepLIFT methods is relatively stable, hence the average absolute error decreases.

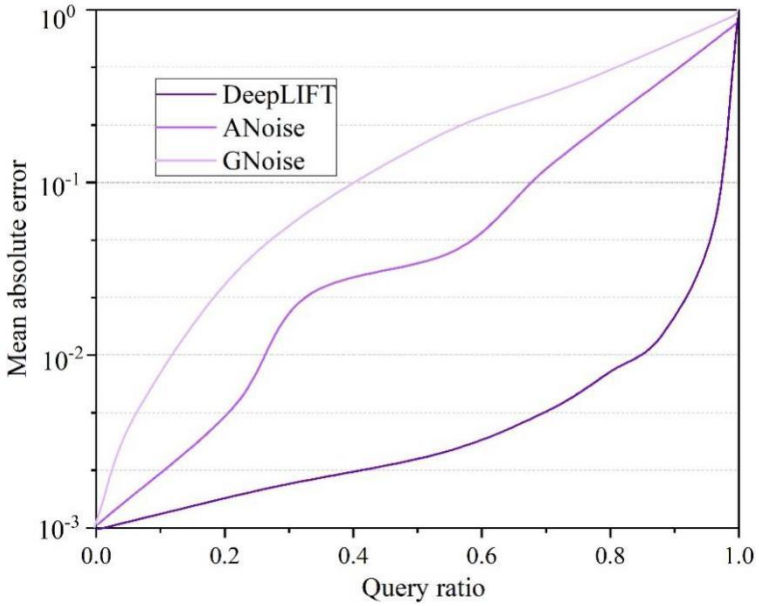

Figure 4: Query ratio affects the performance of each method

2.3.4 The effect of the spatial scale of attribute fetching

Figure 5 shows the effect of the size of the attribute fetch space on the utility of each method. It is clear that the utility of the DeepLIFT method is better than the other methods. In addition, the performance of all methods is relatively stable as the attribute value space size increases. This is due to the fact that all the methods use a fetch space compression method to mitigate the effect of larger fetch space on the query results, which reduces the localized differential privacy noise introduced when local data is collected using the localized differential privacy mechanism.

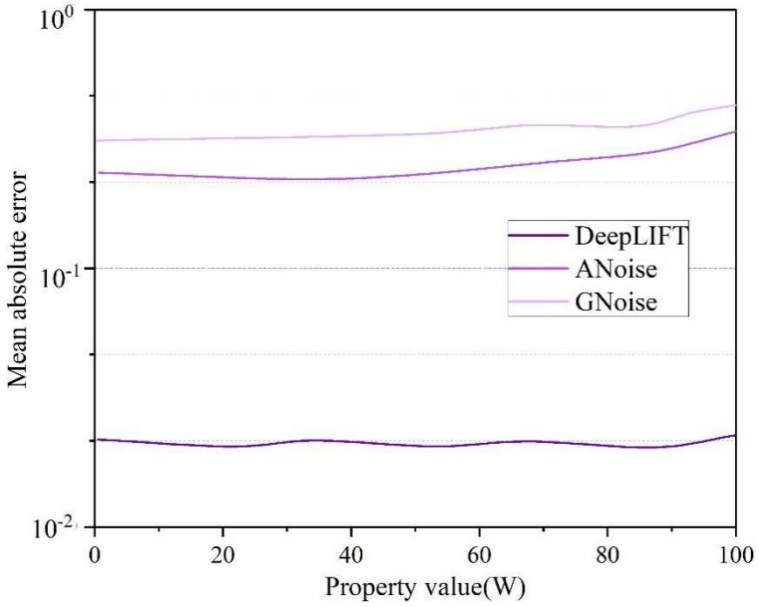

Figure 5: The impact of the attribute value space size on the utility of each method

2.4 Comparative Performance Analysis of DeepLIFT Algorithm

2.4.1 Analysis of the degree of privacy protection

The level of privacy safeguarding in differential privacy is associated with the privacy allowance. We conduct an analysis of how different values of the privacy allowance impact the mean distortion. In this paper, user trajectories are roughly divided into three groups, and the trajectory lengths of 1000-2000, 2000-4000, and 4000-6000 are taken for experimental comparison. In the dataset of this paper, the number of trajectories with a length of 2000-4000 is the largest, and the number of trajectories below 1000 is less so this part of trajectories is not considered.

Table 1 presents the distortion that occurs under various privacy budgets.It is evident that the change in trajectory distortion for different trajectory lengths does not gradually increase, and the distortion of trajectories in the 4000-6000 segment is smaller than that of the 1000-2000 segment, thus indicating that the method in this paper can be applied to longer trajectories with good extensibility.

As the privacy budget increases, the data distortion gradually decreases, which is due to the objective of the scoring function designed by the algorithm in this paper and the nature of the exponential mechanism. The larger the privacy budget the greater the likelihood of selecting the desired result, the better the trajectory is maintained, the scoring function is designed to firstly ensure the privacy of the semantic location. Secondly to keep the trajectory characteristics as much as possible, the trajectory is kept better case, but it will also be more probable to leak the sensitive location, the privacy budget is proportional to the usability, and privacy protection is inversely proportional to this result is in line with the law of differential privacy index mechanism.

Table 1: Distortion under different privacy budgets

Privacy Budget	1000-2000	2000-4000	4000-6000
0.05	0.0261	0.0311	0.0156
0.5	0.0257	0.0265	0.0149
1	0.0218	0.0221	0.0137
5	0.0192	0.0217	0.0126
100	0.0155	0.0189	0.0112
1000	0.0143	0.0148	0.0122

2.4.2 Comparison of running time

To validate the operational efficiency of the algorithm presented in this paper, various distance thresholds are employed to conduct a comparison among three algorithms. The comparison results of the running times of these three algorithms are depicted in Figure 6. The outcomes indicate that the running time of the DeepLIFT algorithm in this paper is longer than that of the other two algorithms. This can be attributed to the incorporation of the intricate MDL algorithm in the mathematical operations of the algorithm in this paper. In an effort to enhance the algorithm's usability and privacy, a certain degree of running efficiency has been sacrificed, leading to relatively low operational efficiency. Nonetheless, the running time of the algorithm in this paper is not significantly longer than that of the other two algorithms. The average running time of the ANoise algorithm is approximately 5.77 seconds, while the running time of the DeepLIFT algorithm in this paper is around 6.34 seconds， which is still within the acceptable range of the sacrificed running efficiency under the need of privacy protection.

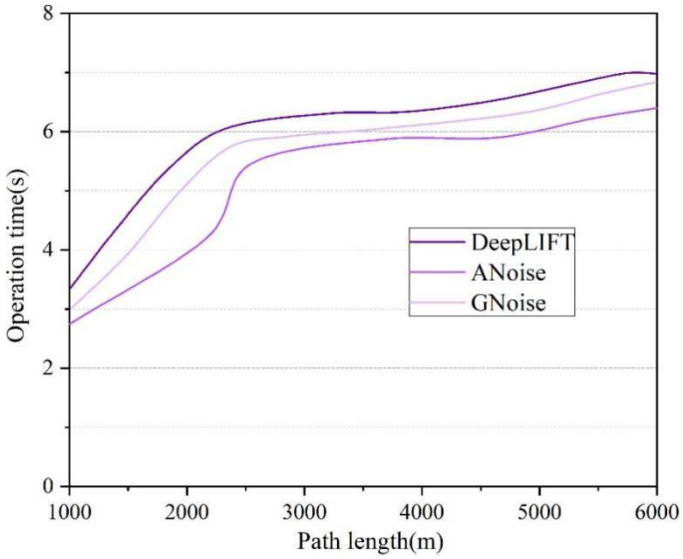

Figure 5: Comparison of running times for the three algorithms

3 Effectiveness of the protection of the individual's right to privacy and the legal challenges and responses to them

3.1 Example Analysis of the Application of DeepLIFT Algorithm for Privacy Protection

Within the realm of medical care, AI models need to deal with a large amount of sensitive data, and privacy protection becomes a key issue. In this study, a pre- and post-test method is used to evaluate the effectiveness of DeepLIFT algorithm in safeguarding privacy. Through a comparison of the alteration in the risk of privacy leakage both prior to and subsequent to the application of the DeepLIFT algorithm, we analyze whether the protection effect of the algorithm on species privacy types meets the predefined requirements. The set requirements for this case are: privacy leakage risk reduction ≥50%.

3.1.1 Methodological design

Pre-test Benchmark: Obtain the benchmark leakage rate for each privacy by modeling the reverse attack test when DeepLIFT algorithm is not used.

Post-test evaluation: Apply DeepLIFT algorithm to identify key features and implement targeted protection, repeat the same attack test.

Evaluation metrics: Use quantitative metrics such as attack success rate, feature reconstruction error, and information entropy change.

Test environment: Deep learning model based on 10,000 simulated medical records of XXX hospital in Province B, including diagnosis prediction and risk assessment indicators.

3.1.2 Pre- and post-test analysis of privacy protection effects

Table 2 presents the outcomes of the pre - and post - tests for five privacy protection effects. These outcomes indicate that the success rate of attacks on the protection of genetic sequence information dropped by 53.78 percentage points,a relative reduction of 270%, and the effect of genetic information protection is significant. In the protection of medical diagnostic records, after adding noise perturbation to the contribution analysis based on DeepLIFT algorithm, the

inference accuracy of medical diagnostic records is reduced to 22.07%, which is a relative reduction of 195% compared to the pre-test results, and the diagnostic information is effectively protected. In the biometric data protection effect, after implementing feature desensitization, the reconstruction MSE increases to 0.63, the reconstruction error increases by 350%, the reconstruction accuracy decreases significantly, and the biometric protection effect is good. In geographic location trajectory protection, the Jekyll and Hyde similarity of location trajectory reconstruction is 0.75, and after applying trajectory generalization processing, the similarity decreases to 0.26, the similarity relatively decreases by 65.33%, and the location privacy protection meets the standard. In socio-economic status protection, the F1 score of socio-economic attribute inference is 0.67, and after applying attribute fuzzification, the F1 score decreases to 0.38, the inference effect decreases by 0.29 percentage points, and the relative decrease is 43.28% < 50%, and its privacy protection effect is not achieved, and the socio-economic information protection effect is insufficient.

Comprehensive analysis found that the protection effect of genetic information, diagnostic records, biometric features and location trajectory exceeds the predetermined standard; however, the protection effect of socio-economic status fails to meet the requirements. It can be seen that DeepLIFT algorithm performs well in recognizing sensitive features with high contribution, and its protection effect is most significant for genetic and diagnostic information; however, socio-economic information is more difficult to protect because of its scattered distribution in the model. Therefore, this paper suggests that a combination of protection strategies can be used for socio-economic information that fails to meet the standard, and a dynamic privacy protection adjustment mechanism can be established to reassess the privacy protection effect periodically.

Table 2: Results of 5 privacy protection effects before and after testing

Private content	Pre-test	post-test	Effect Comparison	Meets the standard
Gene sequence information protection effect	73.54%	19.76%	270%	Yes
Effect of medical diagnostic record protection	65.18%	22.07%	195%	Yes
Biometric data protection effectiveness	0.14	0.63	350%	Yes
Location trajectory protection effect	0.75	0.26	65.33%	Yes
Socio-economic protection effect	0.63	0.38	39.68%	Deny

3.2 Challenges and Countermeasures for the Protection of Individual Privacy Rights in the Internet Age

3.2.1 Obstacles to the Safeguarding of Individual Privacy in the Digital Era

The privacy challenges of the Internet age stem primarily from its “borderless” and “digital” nature. There are three main challenges:

(1) Pervasive Data Collection

Various applications, smart devices and public cameras continuously collect our whereabouts, habits and even biometrics, and the data is generated without the user's awareness.

(2) Precise monitoring and user profiling

Through big data analysis and algorithms, enterprises can accurately portray user profiles and make personalized recommendations and pricing, making individuals nearly transparent in the digital world.

(3) Data Misuse and Leakage Risk

The huge amount of centrally stored data becomes the target of hacker attacks, and the gray industry chain such as illegal use or digital trading by insiders exposes privacy to serious threats of leakage and abuse.

3.2.2 Strategies for the Safeguarding of Individual Privacy Rights in the Digital Era

(1) Strengthen personal protection awareness and techniques

Be cautious about authorization and follow the principle of minimum necessary to share information. Set strong and non-repeating passwords for different accounts, and make sure to enable double verification. Regularly check and clean app permissions, cache and cookies to minimize information leakage at the source.

(2) Make good use of your rights under the law and the platform.

Take the initiative to understand and learn about the rights to know, correct and delete information granted by laws such as the Personal Information Protection Law. When encountering infringement of rights, decisively report through the platform complaint channel or seek legal assistance, defend your rights and interests with actions, and supervise the standardized operation of enterprises.

(3) Enhance information discernment and collective supervision

Cultivate critical thinking, remain vigilant against requests for personal information, and do not easily trust unfamiliar links. At the same time, actively participate in public discussions to monitor corporate data behavior, creating collective pressure to jointly promote the construction of a healthier data ethics code.

(4) Conduct a Comprehensive Enhancement of Remedies for Personal Information

The legal safeguard framework needs to be in harmony with the constantly evolving big - data technology. First, it is necessary to harmonize the regulations regarding personal data protection within the current legal framework. This involves standardizing the concept and categorization of personal data. Simultaneously, an effective integration of administrative, civil, and criminal penalties should be achieved. By doing so, the synergy between public and private law protection can generate the maximum legal effectiveness.Moreover, real - time, full - process supervision should be strengthened. In addition, safeguarding personal data should be incorporated into the scope of public - interest litigation.

(5) Enhance the oversight capabilities of functional departments regarding the safeguarding of personal information.

The authorities ought to enhance both the pre - and post - oversight, and set the reward and punishment standards for the basic business quality of the staff of the infringement review work, so as to realize the connection of the infringement review of personal information protection before, during and after the process. Improve the technical capacity of big data service security and the level of intelligent equipment, and strictly supervise and review from data collection, analysis, emergency disposal to the final use of data.

4 Conclusion

This research paper presents a differential privacy safeguarding approach founded on an adaptive Gaussian mechanism. The aim is to investigate the protective impact on personal privacy during the network age. After that, it outlines the present obstacles encountered by personal privacy and suggests relevant strategies to address them. The findings indicate that:

(1) The DeepLIFT algorithm exhibits excellent extensibility, and its trajectory distortion does not progressively grow as the trajectory length increases. Conversely, as the privacy budget rises, the data distortion gradually diminishes. Although the running time of the

DeepLIFT algorithm is longer compared to the typical comparison model, its operational efficiency remains within an acceptable threshold.

(2) The DeepLIFT algorithm is shown by pre and post-test evaluations to meet the predefined requirements in the protection of most privacy types, this offers a highly effective technological backing for safeguarding the privacy of medical artificial intelligence systems. However, differentiated protection schemes need to be designed for different privacy characteristics and continuously optimized in practical applications.

(3) In the face of the pervasive privacy challenges of the Internet age, individuals can no longer stand alone. Therefore, this paper suggests a tripartite collaboration among "individuals, enterprises and the government" to protect individual privacy. Specifically, individuals need to improve their literacy and actively form their rights, enterprises need to assume the main responsibility of data governance, and governments need to improve legislation and strengthen supervision. Only in this way can we build a solid wall of protection for personal information while enjoying convenience.

About the Author

Kunchi Wang was born in Zhanjiang, Guangdong, China P.R. China, in 1990. He received the Master degree from Guangdong University of Finance & Economics, P.R. China. Now, he is a doctor student Studies in Xi'an Jiaotong university. His research interests include Jurisprudence, Legisprudence.

E-mail: 13376705396@163.com

Baomin Wang was born in Xi'an, Shaanxi, China P.R. China, in 1968. He received the doctor degree from Peking University, P.R. China. Now, he studies in School of law, Xi'an Jiaotong University. His research interests include Jurisprudence, Legisprudence, Comparative Law.

E-mail: baominwang@mail.xjtu.edu.cn

Xingyu Su was born in Shijiazhuang，Hebei.P.R. China, in 1991. He received the Doctor degree from Xi'an Jiaotong University, P.R. China. Now, he studies in Law And Politics School, Lingnan Normal University .His research interest include Jurisprudence, Legisprudence and Judicature

E-mail:suxingyusylvin@126.com

References

[1] Ginosar, A., & Ariel, Y. (2017). An analytical framework for online privacy research: What is missing?. Information & Management, 54(7), 948-957.

[2] Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. Journal of Communication, 67(1), 26-53.

[3] Aswathy, S. U., & Tyagi, A. K. (2022). Privacy breaches through cyber vulnerabilities: Critical issues, open challenges, and possible countermeasures for the future. In Security and privacy-preserving techniques in wireless robotics (pp. 163-210). CRC Press.

[4] Mills, J. L., & Harclerode, K. (2017). Privacy, mass intrusion, and the modern data breach. Fla. L. Rev., 69, 771.

[5] Iman, N. (2024). The fight for our personal data: analyzing the economics of data and

privacy on digital platforms. International Journal of Law and Management, 66(6), 774-791.

[6] Wolofsky, S. (2020). What's Your Privacy Worth on the Global Tech Market? Weighing the Cost of Protecting Consumer Data against the Risk That New Legislation May Stifle Competition and Innovation during This Global, Technological Revolution. Fordham Int'l LJ, 44, 1149.

[7] Niu, Y., Qiu, W., Tang, P., Wang, L., Chen, S., Li, S., ... & Niu, B. (2025). Everyone's Privacy Matters! An Analysis of Privacy Leakage from Real-World Facial Images on Twitter and Associated User Behaviors. Proceedings of the ACM on Human-Computer Interaction, 9(2), 1-38.

[8] Koguchi, T., & Maeda, S. (2022). The economic value of personal information: Analysis of information leakage incidents. In Policies and challenges of the broadband ecosystem in Japan (pp. 213-229). Singapore: Springer Nature Singapore.

[9] Meixiang, L. I. (2020). Research on the Infringement of Citizens' Privacy Rights by Human Flesh Search in China. Asian Journal of Humanities and Social Studies (ISSN: 2321-2799), 8(4).

[10] Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. Communication Research, 48(7), 953-977.

[11] Hamidon, H., Radzi, S. M., Alias, N. R., Arifin, N., & Zukarnain, Z. A. (2022). Personal data abuse: preliminary survey among Malaysian youth netizens. Int. J. Inf. Knowl. Manag, 1, 192-210.

[12] Zhang, Z., & Zang, Z. (2024). ETHICAL ASSESSMENT OF PRIVACY BREACHES IN EPIDEMIOLOGICAL INVESTIGATIONS AND INFORMATION DISCLOSURE IN THE INTERNET AGE: SAFEGUARDING IDENTITY INFORMATION FOR INFECTIOUS PATIENTS. Acta Bioethica, 30(1).

[13] Hyka, D., Hyra, A., Basholli, F., Mema, B., & Basholli, A. (2023). Data security in public and private administration: Challenges, trends, and effective protection in the era of digitalization. Advanced Engineering Days (AED), 7, 125-127.

[14] Huang, L., Zhou, J., Lin, J., & Deng, S. (2022). View analysis of personal information leakage and privacy protection in big data era—based on Q method. Aslib Journal of Information Management, 74(5), 901-927.

[15] Rahim, M. A. A. A., Mohamad, A. M., Kamaruddin, S., & Rosli, W. R. W. (2024, November). Data Leaks Through Public Digital Document Libraries: A Growing Concern in Relation to Personal Data Protection and Cyber Security Regulations. In 2024 7th International Conference on Internet Applications, Protocols, and Services (NETAPPS) (pp. 1-6). IEEE.

[16] Watt, E. (2017, May). The role of international human rights law in the protection of online privacy in the age of surveillance. In 2017 9th International Conference on Cyber Conflict (CyCon) (pp. 1-14). IEEE.

[17] Solove, D. J. (2022). The limitations of privacy rights. Notre Dame L. Rev., 98, 975.

[18] Yan, L. (2024). Research on the legal issues of network privacy right and personal information protection. International Journal of Frontiers in Sociology, 6(5).

[19] Yang, F., & Xu, J. (2018). Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law. Asia & the Pacific Policy Studies, 5(3), 533-543.

[20] Zhu, R., Srivastava, A., & Sutanto, J. (2020). Privacy-deprived e-commerce: the efficacy of consumer privacy policies on China's e-commerce websites from a legal perspective. Information Technology & People, 33(6), 1601-1626.

[21] Creemers, R. (2022). China’s emerging data protection framework. Journal of Cybersecurity, 8(1), tyac011.

[22] Lin, H. (2023). Determination of Infringement in Personal Information Leakage under the Accountability Principle and the Security Principle. Law Sci., 2, 263.

[23] Feng, Y. (2019). The future of China’s personal data protection law: challenges and prospects. Asia Pacific Law Review, 27(1), 62-82.

[24] Guo, Z., Hao, J., & Kennedy, L. (2024). Protection path of personal data and privacy in China: Moving from monism to dualism in civil law and then in criminal law. Computer Law & Security Review, 52, 105928.

[25] Sudarwanto, A. S., & Kharisma, D. B. B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. Journal of Financial Crime, 29(4), 1443-1457.

[26] Syahwami, S., & Hamirul, H. (2024). The Erosion of Privacy in the Digital Age: A Constitutional Challenge in Indonesia. Enigma in Law, 2(2), 75-84.

[27] Sasea, E. M., & Sakmaf, M. S. (2023). Digital bank legal challenges: security protection and leakage of customer personal data. Awang Long Law Review, 6(1), 245-250.

[28] Ayunda, R. (2022). Personal data protection to e-commerce consumer: What are the legal challenges and certainties. Law Reform, 18(2), 144-163.

[29] Toyi, A. R., & Hamidun, E. Z. P. (2025). Establishing Legal Certainty in the Digital Era: Challenges and Solutions. Estudiante Law Journal, 7(2).

[30] Xie, Y. (2024). Legal dilemmas and paths to relief in cross-border transfers of personal data by multinational corporations. Sci. Law J., 3(4), 111-123.

[31] Lundstedt, L. (2018). International jurisdiction over crossborder private enforcement actions under the GDPR. Faculty of Law, Stockholm University Research Paper, (57), 50.

[32] Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. Journal of cybersecurity, 4(1), tyy001.