Mo Chen* and Jens Grossklags

# An Analysis of the Current State of the Consumer Credit Reporting System in China

**Abstract:** The Chinese Social Credit System (SCS), known as the first national digitally-implemented credit rating system, consists of two parallel arms: a government-run and a commercial one. The government-run arm of the SCS, especially efforts to blacklist and redlist individuals and organizations, has attracted significant attention worldwide. In contrast, the commercial part has been less often in the public spotlight except for discussions about Zhima Credit.

The commercial arm of the SCS, also referred to as the Consumer Credit Reporting System (CCRS), has been under development for about two decades and took a major step forward in 2015 when 8 companies were granted permission to implement pilot consumer credit reporting programs. This development fundamentally increased the reach and impact of the SCS due to these companies' sizable customer base and access to vast troves of consumer-related information.

In this paper, we first map the Chinese CCRS to understand the actors in the credit reporting ecosystem. Then, we study 13 consumer credit reporting companies to examine how they collect and use personal information. Based on the findings, we discuss the relationship between the CCRS and the SCS including the changes in the power relationships between the government, consumer credit reporting companies and Chinese citizens.

**Keywords:** Social credit system, Consumer credit reporting, Privacy policy, China

DOI 10.2478/popets-2020-0064
Received 2020-02-29; revised 2020-06-15; accepted 2020-06-16.

## 1 Introduction

The Chinese Social Credit System (SCS) is the first national digitally-implemented credit rating system encompassing companies, individuals, public and government institutions, and the judicial system [53]. According to the Chinese government, the goal of the SCS is to "allow the trustworthy to roam everywhere under heaven while making it hard for the discredited to take a single step" [42, 53]. Yet, after 5 years of effort, there is still not a unified SCS nationwide. Instead, the construction and implementation of the SCS continues to evolve at multiple levels.

As noted in previous research, the SCS consists of a government-run part and a commercial one [34, 36]. The government-run SCS is known in particular for its implementation of blacklists (recording "bad" behavior) and redlists (recording "good" behavior) as well as its joint reward and punishment mechanism. Blacklists and redlists publish personal information and behaviors to serve public shaming and praising purposes, respectively. The joint reward and punishment mechanism is implemented on the basis of cooperation between different government authorities. One of the most typical cases relates to individuals, who fail to repay debt, and are subsequently included in blacklists with their personal information for public shaming purposes and banned from taking high-speed trains and flights (e.g., [32]). Such examples have triggered numerous debates in the media as well as in academia. In particular, privacy is widely regarded as a major concern raised by the system [13, 15]. So far, media reports and public discussion that consider the SCS as a threat to privacy (e.g., [8, 46]) and even compare the system to Orwell's *1984* have paid predominantly attention to the government-run SCS which is mandatory for all Chinese citizens. In contrast, the privacy implications and risks associated with the commercial arm of the SCS, despite some focus on specific cases (usually Zhima Credit), are hardly explored in any systematic way.

Basic SCS concepts such as blacklists and redlists are well known to Chinese citizens as they are related to past propaganda practices and widely publicized in the media. As such, it is perhaps less surprising that the Chinese public has been reported to be relatively unconcerned about the government-run SCS [31]. However, Chinese citizens are likely much less familiar with the detailed processes of the government-run SCS as it

***Corresponding Author: Mo Chen:** Technical University of Munich, E-mail: mo.chen@tum.de
**Jens Grossklags:** Technical University of Munich, E-mail: jens.grossklags@in.tum.de

is not of particular interest to the public to follow the rapidly evolving SCS-related government policies [44].

In addition, the majority of the Chinese are very familiar with popular apps such as Zhima Credit and JD Finance offering commercial consumer credit reporting services, which are – on a high level – comparable to products that Equifax, Experian, and TransUnion provide in the U.S., and which are also reliant on the collection and processing of vast amounts of consumer (credit) information [38]. In fact, in China, the commercial arm of the SCS, the Consumer Credit Reporting System (CCRS), can be considered to be of higher every-day relevance to the public (see Section 4). At the same time, the CCRS is less systematically discussed in the media and research. Our work addresses this literature gap by making the following contributions. First, our research maps the current status of the CCRS through an analysis of publicly available documents. Second, we study consumer-facing (privacy) policies of the key entities in the CCRS to better understand their likely impact on privacy and data protection in Chinese society. Third, we discuss the relationship between the CCRS and the SCS including the changes in the power relationships between the government, consumer credit reporting companies and Chinese citizens.

The CCRS follows a tightly regulated licensing model, such that there are not many companies conducting business in this field. Given this situation, we enlarged our study scope to include a relatively broad set of 13 commercial credit reporting companies (see Section 4) with ties to the CCRS based on government documents and observed practices.

## 2 Related Work

Credit reporting such as consumer reporting agencies (for example, in the U.S.) have a long history [45]. While it is widely acknowledged that an individual's previous loan performance may serve as a predictor for future behavior in the financial context, data collection and use associated with credit reporting are not undisputed. In particular, the associated privacy issues have been subject to academic research.

Several key issues emerge, which are at the intersection of transparency and privacy. For example, due to limited information it is unclear to which degree data collected and used by credit reporting agencies is accurate [24]. Further, the concrete algorithms to calculate credit scores are generally considered proprietary information even though the general building blocks may be known. Such information asymmetries are particularly worrisome outside of tightly regulated contexts [51].

Perhaps the most comprehensive review effort in this problem context is a work by Jentzsch who conducts an international comparison of credit reporting and privacy implications [29] with a particular emphasis on economic and regulatory issues. But her book predates the recent development of the SCS and CCRS.

A variety of studies focus on the mechanisms and assessment of the government-run SCS in China, providing a high-level overview and mapping its development [18, 20]. Some empirical research also sheds light on the commercial arm of the SCS. For example, Ohlberg et al. issued a report examining the public portrayal of the SCS, which draws on a comprehensive collection of official Chinese news media articles and official communications [44]. They also questioned the role of the commercial entities within the SCS ecosystem. Perhaps surprisingly, matters of data protection or privacy, more generally, are rarely discussed in these sources, while other factors with user-centric relevance are often part of online discussions, e.g., how to get ahead within the system and to gain higher scores in the commercial offerings with SCS relevance [44].

In addition, several social science and legal research works discuss the privacy and surveillance implications of the SCS. One key finding is that due to the lack of a comprehensive legal system to protect privacy, the SCS is able to collect, process, and analyze personal data for a broad range of different purposes, which might undermine privacy [13].

The surveillance tradition of the SCS is dating back to the personal file (dàng'àn) system, which archived individual's private life in detail [39]. Different from the traditional surveillance system, however, the SCS is designed to cover wider aspects of societal life [34] and as a critical pathway for the Chinese government not only to monitor, but also to regulate and shape people's behaviors using information technology as a political instrument [40]. The construction of the SCS involves significant cooperation between different government departments in China and also calls for an increasing participation of large technology companies [63]. For example, the high-tech giant Baidu provides technical support to build and maintain the national platform of the SCS "Credit China (信用中国)" (https://www.creditchina.gov.cn/) [33], which informs the public about all SCS developments. The integration of public and private sector actors in big data-enabled surveillance is developing a "corporate-state nexus" (as termed by Ball and Wood), which blurs the boundaries between the government and commercial sectors [5].

In summary, relatively few papers comment specifically on the *commercial arm* of the Chinese Social Credit System, and to the best of our knowledge, we are unaware of any empirical research examining the evolving privacy practices in the CCRS.

## 3 Research Methods

For this research, we collected different first-hand materials from SCS and CCRS entities, as well as articles from secondary sources to conduct a document analysis mapping out the development of the CCRS in China. More specifically, our research relies on relevant instances of three types of documents: government documents, credit reporting companies' websites and various media resources.

Government documents such as laws, regulations and reports enhance our understanding of the high-level development roadmap for the CCRS and privacy protection in China. Company websites represent a primary source to explore the background, the stakeholders, consumer-oriented (privacy) policies, as well as product information and services of the company. In addition, media resources can be helpful supplements, especially those with interviews with companies' representatives. We only focused on news reports which are released by well-established media outlets. The first two types of documents are in Chinese, while media resources used in this research include both Chinese and English sources.

To study the privacy-related documents of companies within the Chinese CCRS, we repurposed the taxonomies constructed for *Polisis* (https://pribot.org/polisis/), which is a machine-learning-trained tool for the analysis of privacy policies. *Polisis* utilizes eight taxonomy categories that cover the most important issues encountered in consumer-oriented privacy policies (see Table 10) [22]. However, the *Polisis* tool itself cannot be used to analyze privacy policies in Chinese. Given the small number of privacy-related documents from the Chinese CCRS, it is reasonable to manually analyze the documents under the framework of *Polisis*.

For our purposes, we modified the taxonomies from three perspectives to build an annotation template (see Table 2). First, we further divided the taxonomy category of "data collection" into "personal sensitive information" and "other information". The distinction between the two types of data is based on the definition and examples provided by the *Information Security Technology – Personal Information Security Specification* (referred as *Personal Information Security Specification* for short in this paper) [21], which is a new data protection standard in China. According to the standard, personal sensitive information refers to information that once disclosed, illegally provided or abused may cause harm to persons or property, and may lead to damage to reputation and physical and psychological health, or discriminatory treatment. Based on the categories and examples that the *Personal Information Security Specification* provides, we identified eight types of "sensitive personal data" in the template. Secondly, we added as a new taxonomy category "special purposes of data collection, usage and sharing" to capture any purposes beyond providing services and marketing. Thirdly, we merged "your choices" and "right to edit" into "right to edit and correct" which investigates the user's right to edit, remove and dispute records about his/her personal data. Once we updated the template with these changes to the taxonomies (see Table 10), we developed tailored detailed items for each of the taxonomy categories.

We collected all privacy-related documents in November 2019. To make sure the analysis is robust, we developed the template in an iterative manner. One researcher first generated an initial version of the template, and used it to code three policies to test the fit of the template and to highlight any encountered problems. Then, we had a discussion to resolve the problems, improved the template, and tested the new template with another three policies. This iterative process proceeded for three rounds until the team agreed on the final version of the template which contains 30 items designed for the eight taxonomy categories. We provide a sample of the coding to exemplify our current practices in Table 13 in the Appendix. We also followed a protocol that standardized the procedures for analyzing each policy. Two researchers, who are Chinese native speakers, coded the policies independently. The first round of coding resulted in disagreement of 6 out of the 270 items (2.22%). The disagreement rate was low as the coding is not complicated but predominantly about checking the existence of specific content. We then reconciled the results and revised the coding results in a collaborative manner.

## 4 Mapping the Chinese CCRS

The credit reporting system came into existence in China in the late 1980s, starting with the enterprise credit reporting service [30]. In particular, the development of the CCRS was initiated with the establishment of the Shanghai Credit Information Services Co., Ltd. in 1999, which was part of an initial pilot of SCS construction in Shanghai [35]. Following the directives about SCS construction set out in the 16th National Congress of the Communist Party of China (CPC) and the Third Plenary Session of the 18th Central Committee of the CPC in 2002, the People's Bank of China (PBoC) started in 2004 to build a national centralized CCRS, which was then launched two years later.

By 2014, 1,811 entities had been connected to the consumer credit system of the Credit Reference Center (CRC). 83% of the collected data were about credit records and credit accounts, while other information including social insurance, the provident fund payment, and information about telecommunication and tax accounted for 17% [16]. Although the CRC's data from 2014 covered a population of 857 million, only 350 million of them had a credit record. Therefore, the coverage rate of consumer credit records was only 35%[1], which was far lower than, for example, in the U.S. (92%) [23]. The development of the CCRS was accelerated after 2014 when the State Council issued the *Planning Outline for the Construction of a Social Credit System (2014-2020)* to promote overall construction of the SCS [53].

Fundamental progress was made in 2015 when a series of substantive actions were taken. The PBoC released the *Notice on the Preparation of Personal Credit Information Service* at the beginning of the year. Following this *notice*, 8 commercial companies (Zhima Credit, Tencent Credit, Qianhai Credit, Pengyuan Credit, China Chengxin Credit, IntelliCredit, Sinoway Credit and Koala Credit) were granted *permission* to run consumer credit services, which served the purpose to implement pilot SCS programs and fostered the marketization of the CCRS in China.

The 8 commercial companies, however, failed to receive individual *licenses* after a two-year trial period. Instead, in 2018, these companies, together with the National Internet Finance Association (NIFA), which is a state-level organization, established Baihang Credit which received the first *license* to run a consumer credit service. As such, Baihang Credit is the only company that is fully licensed to run a consumer credit reporting service. But there is no clear evidence that any of the 8 companies completely discontinued their previously developed services.

In fact, the national platform of the SCS provides access to 10 commercial companies for requesting consumer credit scores: Zhima Credit, Tencent Credit, Qianhai Credit, Pengyuan Credit, China Chengxin Credit, Sinoway Credit, JD Finance, Du Xiaoman Credit, Wanda Credit, and China Youth Credit. The first 6 companies were participants of the pilot SCS programs discussed above. However, in total, there are currently 13 companies operating in the CCRS in China, which are all covered in the discussion in this paper.[2]

In the following, we begin with a detailed analysis of the 13 entities that are currently providing commercial credit services. To aid in our analysis, we reuse a classification made by Huang et al., who divided the business models of the 8 pilot companies, which were in the first round of marketization, into three categories: (1) traditional credit rating companies, (2) internet and financial giants, and (3) other emerging institutions [28]. We use this classification for our set of 13 companies. Our analysis is focused on five perspectives: Who are the *stakeholders*? What *data resources* are used? What *calculation dimensions* are stated for the scores? What *algorithms* are being used? And what are the stated *application areas* of the scores?

Understanding the diverse building blocks of the CCRS including participants and data processing in more detail is a crucial prerequisite to also better assess the associated potential privacy implications.

## 4.1 Traditional companies

Pengyuan Credit, China Chengxin Credit and IntelliCredit are 3 old brands in China's credit market with a relatively long history in the area of enterprise credit. Pengyuan Credit has strong governmental affiliations as it used to be held by the municipal government of Shenzhen, but was recently reorganized and is now owned by several legal and natural persons (see Table 1). China Chengxin Credit belongs to China Chengxin Group (CCX), which was the first national credit rating agency in China. IntelliCredit is a private third-party company and, according to the company's webstie, has contributed to the infrastructure construction of the Chi-

[1] Population aged between 15 and 64 was taken into consideration in the calculation.

[2] In addition to Baihang Credit, there are the 8 companies which ran the pilot SCS programs between 2015 and 2017, plus 4 additional entities which are listed on the national platform.

nese credit reporting system during the past decade. These 3 companies do not generate data themselves but have stable and wide access to data from business partners and public institutions. Pengyuan Credit develops Tianxia Xinyong, which is a platform providing credit reports and scores (Tianxia Score) to both enterprises and individuals. China Chengxin Credit offers Wanxiang Score to individuals. IntelliCredit provides consumer credit scores directly to any companies (but not directly to individuals; however, authorization is required).

Contractual capacity, identity quality, credit history, and behavioral characteristics are four important financial evaluation dimensions for scoring and rating individual's creditworthiness and are taken into account by all different types of consumer credit reporting companies (see Tables 1, 11 and 12). Contractual capacity emphasizes personal assets and income; identity quality refers to personal identity information such as education and working experience; credit history is about repayment records and default records; behavioral characteristics examine individual's online and offline behavior such as voluntary work. In addition to these four basic criteria, other evaluation dimensions are considered as well. Not all companies explain even the broad calculation dimensions, and specific terms used in the statements about calculation dimensions are often not sufficiently documented. For instance, Pengyuan Credit refers to "public evaluation" in the consumer credit score [1], which remains unexplained.

In the internet financial era, these traditional companies make efforts to transform themselves with the help of information technology and big data methods to be internet-based as well. In addition to traditional statistical methods, all 3 companies now use advanced algorithms such as big data mining and machine learning to process data; and China Chengxin Credit takes the individual's social network into consideration in consumer credit reporting.

The application of the consumer credit products from traditional companies largely remains in the financial area. But the use of Tianxia Score is more similar to that of the internet and financial giants as it is now expanding to diverse areas of e-commerce, online social networking, apartment rental and job hunting.

## 4.2 Internet and financial giants

Zhima Credit, Tencent Credit, JD Xiaobai Credit, and Panshi Xiaomanfen are developed by Ant Financial, Tencent Financial Technology, JD Finance and Du Xiaoman Financial, respectively. These four financial companies are affiliated to Alibaba, Tencent, JD.com and Baidu, which are four internet giants in China specializing in the areas of online shopping, online social networking, online entertainment and online search, respectively. Qianhai Credit is a wholly owned subsidiary of Ping An Insurance, which is one of the largest insurance companies in China. With such a background, these companies enjoy the advantage of larger and more diversified databases constructed by their parent companies. For example, Zhima Credit and JD Xiaobai Credit can draw on a large amount of data about online shopping. Tencent Credit may refer to data generated from Tencent services related to online social networking, entertainment and transactions. Du Xiaoman Financial likely has access to Baidu's data about individuals' online behaviors. Qianhai Credit could rely on offline and online consumer data from Ping An Insurance. Further, these internet and financial giants lead innovations not only in algorithms, but also in the development of calculation dimensions by including new factors such as online behaviors and online social networking (see Table 11).

Using the additional information about individuals and big data technologies, these companies are able to develop scores for creditworthiness of those who do not have financial records, but exhibit varied online behaviors. For example, the number of yearly active users of mobile apps for Taobao and Tmall, which are both subsidiaries of Alibaba reached 755 million by the end of June 2019 [3]. What an individual buys online may have little to do with creditworthiness. But it makes more sense when this information is combined in the analysis with many other types of data such as voluntary work records, which are also available in Alibaba's database.

With a strong background in such fields as internet and finance, these companies have expanded the application of consumer credit scores beyond the financial area to online and offline consumption as well as some public services (see Table 11). It is common for individuals with a high credit score provided by these companies to enjoy discounts, "pay later" services[3], and deposit-free rental for products and services provided by the companies and their business partners. Meanwhile, the credit scores can also be used in some public service contexts such as visa applications and health

[3] This means the individual can use a product or service free for trial and only pays when he/she is satisfied with it.

| Consumer Credit Score | Company | Stakeholders | Data Resources | Calculation Dimensions | Algorithms | Application Areas |
|---|---|---|---|---|---|---|
| **Tianxia Xinyongfen/天下信用分(320-800)** | Pengyuan Credit (鹏元征信) | Seven legal persons and several natural persons | National and local governments, public institutions; Business partners | 1. Income capacity; 2. Asset and property; 3. Identity quality; 4. Behavioral practices; 5. Credit history; 6. Public evaluation | Traditional mainstream model, big data mining and modelling | Finance; E-commerce; Social network; Apartment rental; Job hunting |
| **Wanxiang Score/万象分(300-900)** | China Chengxin Credit (中诚信征信) | CCX Group (中诚信集团) | Public institutions, business partners, telecommunication operators | 1. Identity qualities; 2. Contractual capacity; 3. Social network impact; 4. Behavioral characteristics; 5. Credit history | Traditional scoring-card model and machine learning | Finance |
| **N.A.** (No name for the score) **(500-900)** | IntelliCredit (中智诚征信) | Private third-party company | Business partners, other third party institutes | 1. Level of activity about individual's credit; 2. Contractual capacity; 3. Credit history; 4. Identity qualities; 5. Ability of credit consumption | The unique technology of approximate string matching for Chinese; Clique algorithm | Finance |

**Table 1.** Traditional credit companies in China. The shareholder information is from the companies' websites and Tianyancha (https://www.tianyancha.com/) which is a large data technology service company with a vast repository of Chinese enterprise information. Tianyancha's service is now only accessible in China. Information for data resource, algorithms, calculation dimensions and application areas is based on the companies' websites, a BCG report [23] and the Chinese official media outlet "people.cn" (http://history.people.com.cn/peoplevision/n/2015/0731/c371452-27391634.html).

care. For instance, according to the app of Zhima Credit, Canada and Latvia accept Zhima Credit reports as financial statements in visa applications if individuals' Zhima Credit scores are over 750 and 700, respectively. Zhima Credit is also introduced to the health care area in Shanghai which is one of the most developed cities in China, so that patients whose Zhima score reaches 650 can make an appointment through the app of Alipay and do not have to make any payment until the end of the medical treatment[4].

## 4.3 Others

The remaining 5 companies have more diverse backgrounds (see Table 12). With the first license in the area of consumer credit service, Baihang Credit started to serve the market in 2019. But it remains unclear which type of consumer credit service it provides, what its data resources are, how it calculates credit scores, and in which areas the credit scores can be used. The shareholder structure indicates a broad access to a wider range of databases. However, the status of data sharing between the different shareholders and Baihang Credit at the operational level is not fully explained. For instance, the general manager of Zhima Credit explicitly told the media that there is no data sharing between Zhima Credit and Baihang Credit [12].

Wanda Credit is affiliated with Wanda Group which covers a wide range of businesses such as real estate, culture and finance. There is little information available about Wanda Credit as the company's official website was not accessible during our research period between August 2019 and March 2020. It stopped providing enterprise credit services by the end of 2019, but the state of consumer credit services is unclear. China Youth Credit is affiliated with Tsinghua Unigroup which is China's top state-backed chip maker. Different from other companies, it develops the app Unitown specifically targeting the youth in China. Sinoway Credit is set up by four large financial companies of which Shenzhen InfoTech Technologies is dedicated to providing financial technologies to banks and Qingkong Sanlian (清控三联) is wholly owned by PBoC School of Finance, Tsinghua University. The 100% shareholder of

[4] Usually, patients in China have to make payment several times (e.g., for different types of medical investigations and treatments) during the medical treatment. Refer to *Xinhua News* at http://www.xinhuanet.com/tech/2017-11/08/c_1121924052.htm.

Koala Credit is Lakala Credit Management, which is the market leader in intelligent point-of-sale (POS) systems. These different credit services rely to a large degree on the respective company's cooperation partners to get access to data. For instance, Koala Credit's partners include UnionPay and the five largest commercial banks in China, and China Youth Credit shares data with the State Information Center and many local governments based on its state-owned holding background.

Similar to the other two groups of companies, these *other* companies adopt advanced IT technologies to process data. Calculation dimensions for credit scores vary due to the differences between their databases (see Table 12). As mentioned above, Lakala Credit Management specializes in intelligent POS systems and thus takes transaction data into account. China Youth Credit operates the platform of Volunteers in China (https://zyz.org.cn) and thus pays attention to individuals' volunteer work as well. In terms of credit score application, these companies step into the fields of consumption, job search, and apartment rental.

One can observe that about half (6 out of 13) of the companies have e-commerce as a key application area of the credit score. For example, the credit services provided by the commercial companies connect the CCRS with the sharing economy as shared products can be easily provided at different prices based on different credit ratings. Given this situation, credit scores from these commercial companies have been interpreted as transforming creditworthiness to loyalty to their services [17, 44]. But such an interpretation is insufficient as financial service and public service remain the focus of the Chinese CCRS. It is more adequate to say, in our opinion, that the commercial companies expand the understanding of credit scores and broaden the scope of the application areas of such credit scores. This process is fostered by internet giants' active participation in the consumer credit reporting industry and the growing internet penetration rate which reached 64.5% by March 2020 with an internet population of 904 million [14].

The universal access to the internet provides rating-relevant evidence other than credit records from banks, which is of particular significance to the one-third of Chinese individuals who do not have any credit records [60]. At the same time, the broader use of the internet in people's daily lives results in pervasive digital footprints and raises increasing concern about privacy in Chinese society. According to Cunzhi Wan, director-general of the Credit Information System Bureau, PBoC, one of the three key reasons why none of the 8 companies were granted a license for the consumer credit reporting service is the unprecedented demand from the public for privacy protection [62].

Previous work has observed that the SCS as a whole has the potential to collect, process, and analyze personal data for various purposes due to the growing popularity of online services and the lack of a comprehensive legal system [13, 25, 47]. Our analysis above provides insight regarding the overall scale and focus of the CCRS. An investigation of the detailed privacy practices within the CCRS is however also crucial, which is the focus of the following section.

# 5 Privacy Policy Analysis

The focus of our analysis is on the self-reported privacy practices as evidenced by consumer-oriented (privacy) policies of the companies involved in the CCRS. We investigate the accessibility of the policies as well as their contents with the aid of the developed taxonomies.

## 5.1 Privacy policy accessibility

Unless a privacy policy is easily accessible to users, the content of the policy is less meaningful. From the legal perspective, the *Internet Security Law* which came into effect in 2017 to achieve progress in promoting data protection includes a "right of personal information" and states the requirement to publish the rules, the purposes, the way and the scope of data collection and usage. But the *Internet Security Law* lists principles only and does not provide more detailed requirements. The *Personal Information Security Specification* which came into effect in May 2018 with wider, innovative and much more detailed definitions and requirements on various perspectives of data protection, also requires the personal data controller to develop a privacy policy and has specific requirements on the policy's content. The *Personal Information Security Specification* is (by some) even referred to as the Chinese version of the EU General Data Protection Regulation (GDPR) due to its complex and high-standard requirements in data protection. But a critical difference is that it is merely a recommended standard and thus lacks power. In terms of privacy policy accessibility, we examined (1) the existence of a privacy policy and (2) how easy it is for users to find the policy.

After careful searching and examination, we obtained the privacy policies from 7 of the 13 companies

(53.8%). 4 of these 7 (57.1%) privacy policies are specifically for the consumer credit service: Tianxia Xinyong, IntelliCredit, Zhima Credit and Koala Credit. The other 3 policies broadly cover different services from the company (JD Finance, Tencent Credit and Qianhai Credit). We found two documents for privacy protection for Ping An Insurance, titled "Privacy statement" and "Protecting your privacy", respectively. In this case, we include both of these two documents into our analysis for Qianhai Credit.

Du Xiaoman Financial issues three privacy policies for three out of five types of products and services. For the Panshi Xiaomanfen which is provided as part of the "Financial Technology" service, however, we could not locate a privacy policy. Instead, the company explains at the bottom of the main page that "Du Xiaoman Financial provides service only when the merchant provides legal and valid user authorization. The merchant provides user's identity information and Du Xiaoman Financial provides a service of feedback verification. The service content does not involve the user's original private information".[5]

We also tried to identify any other materials that might shed light at the privacy practices of the companies. Even in this case, however, we did not find any related files for Sinoway Credit, Baihang Credit and Wanda Credit[6] after examining the companies' websites carefully and using both Google and Baidu search engines with different keywords. But we located two terms of service documents for China Chengxin Credit and China Youth Credit, respectively. In order to expand the analysis scope, we included the two *terms of service* documents into our analysis as well.

When present, the privacy policy is usually available at the bottom of the main page; except for Koala Credit which we obtained through Google search with the keywords "考拉征信 隐私政策" (Koala Credit privacy policy). The "Privacy statement" for Ping An Insurance is presented with a link at the bottom of the main page while the "Protecting your privacy" document is available in the sub-page of "online sales". Terms of service documents for China Youth Credit and China Chengxin Credit are both available on the registration page.

In terms of the privacy policy's structure, all the internet giants and Koala Credit frame their policies in a similar way, i.e., they are containing detailed information about data collection, usage, sharing, storage and rights of users, etc. In contrast, the privacy policies for IntelliCredit and Qianhai Credit are less informative about how the company collects and uses data. In fact, the privacy policies from these 2 companies explicitly state that they apply only to the materials collected through the companies' websites, indicating that the companies may collect a wider range of data in other ways or from other sources than presented. The two terms of service documents from China Youth Credit and China Chengxing Credit contain some information about data collection and usage, but are not specifically about privacy practices.

In total, the analysis of privacy policy or terms of service documents in this paper covers 9 out of the 13 (69.2%) companies due to limited availability. In the following subsections, we go through the eight modified taxonomy categories in detail.

## 5.2 Data collection

4 out of 9 (44.4%) companies use the term "personal information" with neither explanation nor specification of different types of "personal information". It is unclear if the term is used as it is defined by the *Personal Information Security Specification* (see Section 3) or in a narrower sense. In this case, we consider the specific category of "data collection" as unclear unless there is further information provided for reference. In general, as Table 2 shows, internet giants state rather clearly whether they collect specific information or not while traditional companies are less transparent about data collection.

*Sensitive information* is collected by all of the 9 (100%) consumer credit reporting companies. But the types of sensitive information they collect are different (see Table 2). *Personal identity information* is about the basic information of a natural person, such as name, date of birth, gender, home address, identification number, which is usually included in the ID card, passport, driving license and social security card. Such information is explicitly listed in the data collection scope in the privacy-related documents from 7 out of 9 (77.8%) companies.

We also attempted to make a distinction between "we will" and "we may" in data collection. Based on the variety of statements across different companies, we

[5] The original note in Chinese: "度小满金融仅在商户提供合法有效用户授权的前提下提供服务，由商户提供用户身份信息，度小满金融反馈验证服务，服务内容不涉及用户原始隐私信息."

[6] The website for Wanda Credit was not accessible during our research period from October 2019 to June 2020.

| | Traditional companies | | | Internet and financial giants | | | | Others | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Tianxia | China Chengxin | Intelli-Credit | Zhima | Tencent | JD Finance | Qianhai | Koala | China Youth | "Y"s |
| **Sensitive data** | | | | | | | | | | |
| Identity info | Y | U | U | Y | Y | Y | Y | Y | Y | 7 |
| Financial info | Y | Y | U | Y | Y | Y | U | Y | Y | 7 |
| Health info | U | N | U | N | Y | U | U | U | N | 1 |
| Biometric info | Y | N | U | N | Y | Y | U | Y | N | 4 |
| Contact info | Y | Y | U | Y | Y | Y | Y | Y | U | 7 |
| Current location | Y | U | U | U | Y | Y | U | Y | U | 4 |
| Online activity | Y | U | Y | Y/N | Y | Y | Y | Y | U/N | 7 |
| Non-publicly disclosed info | Y | U | U | U | U | U | U | U | U | 1 |
| **Other data** | | | | | | | | | | |
| Info of personal contacts | U | U | U | U | Y | Y | Y | Y | U | 4 |
| Device info | Y | U | U | Y | Y | Y | U | Y | Y | 6 |
| Publicly disclosed info | Y | U | U | Y | U | U | U | Y | Y | 4 |

**Table 2.** Annotation results: Data collection. "Y" for "Yes": the policy states explicitly that the company will collect such information; "Y" in *pink*: the company collects such information for sure; "Y" in *blue*: the company possibly collects such information; "N" for "No": the policy states explicitly that the company will not collect such information; "Y/N" for both "Yes" and "No": the policy states explicitly that the company will collect certain type(s) of the information and will not collect some other types of the information; "U/N" for both "Unclear" and "No": the policy states explicitly that the company will not collect certain type(s) of the information, but does not mention if it will collect other types of the information; "U" for "Unclear": the policy does not mention this issue. The code "U" represents the same for following tables (Table 3 to Table 9).

developed the categories as follows: "we will" includes statements such as "you authorize our company to collect your data when you are using related services", "we need to/will collect...", "we collect...", etc.; "we may" includes statements such as "we may require you to provide the information". In our sample, 6 companies collect personal identity information while Tencent states that it may collect such information. The terms of service document of China Youth Credit uses "personal information" in parallel with other types of information such as "device information" and "asset information".

*Financial information* represents the individual's financial status, e.g., bank savings, property information, credit history, bank statement and virtual transaction data, etc. which are all closely and directly related to an individual's creditworthiness. It is collected by 6 companies and may be collected by Tencent (77.8% in total).

The *Regulation on the Administration of the Credit Reporting Industry* states explicitly that credit reporting companies are not allowed to collect information about religious beliefs, genetic data, fingerprints, blood type, diseases and medical records. One third of the companies include this statement explicitly in their privacy-related documents (see Table 2). Tencent is the only one that may collect *health information* which could be medical records, disease, diagnose and treatment information or a family medical history. According to the Tencent privacy platform, the term "personal sensitive information" is linked directly (by clicking) to another section "name/term explanation (名词解释)" in which both health information and biometric information are included. The *biometric information* that might be collected by 4 companies include facial recognition characteristics, iris, fingerprint and hand contour.

*Contact information* which includes email address, telephone number and home address is collected by 7 (77.8%) companies. *Current location information* refers to positioning and tracking information. It is/may be collected by 4 (44.4%) companies.

*Online activity information* covers a wider range of individual behavior such as web browsing, online shopping, transactions and online chat. This type of information is collected through the use of various tracking technologies such as cookies and fingerprinting by all companies except China Chengxin Credit which does not mention this issue in its terms of service. Again, Tencent states that it may collect such information. Zhima Credit and China Youth Credit make a distinction between different types of online activities and state in their privacy policies that they will not collect data from online chats or views on social media. But it is unclear if China Youth Credit collects other types of online activity information.

Tianxia Xinyong is the only company that collects *non-publicly disclosed information* which is usually generated from services provided by the government or public institutions. As public institutions are important data sources for most consumer credit reporting companies (see Tables 1, 11, and 12), it is likely that CCRS companies collect non-publicly disclosed information based on special ties with public institutions. For instance, although not explicitly stating whether collecting non-publicly disclosed information or not, China Youth Credit mentions explicitly that it collects data from government public information platforms and all types of public institutions.

*Other information*: We discuss three other types of personal information that are widely collected by consumer credit reporting companies (see Table 2). We find that 3 companies collect *information of personal contacts*, such as the address book, and Qianhai may also collect such information (44.4% in total). *Device information* such as computer, cell phone brands, software, device context and network context is collected by 6 companies including Tencent which may collect such information. *Publicly disclosed information* refers to all different types of information that is publicly available such as the blacklist records released by courts in the government-run SCS. Such information is collected by 3 companies and may also be collected by Koala Credit.

## 5.3 Third-party sharing

We found that only JD Finance and Koala Credit provide some information about what is going to be shared with a third party (see Table 3), including transaction information, service information, user account information, location information and device information. Also, these two companies list the types or give examples of the third-party companies. In all the other 7 (77.8%) policies, "personal information" or "your information" is used in the section about third-party sharing without any specification.

All companies except 2 traditional ones which do not mention the issue of data sharing state the necessity of consent requirement for data sharing. At the same time, they also include the situation in which the company may share user's information without consent requirement, such as for the purposes of providing products and services, protecting personal information and some special purposes (see Section 5.4). In particular, Zhima Credit illustrates that data sharing takes place to the extent permitted under law, *public order and morality*, but does not provide further explanation. In general, traditional companies are less transparent in data sharing in their privacy-related documents.

| | Traditional companies | | | Internet and financial giants | | | | Others | |
|---|---|---|---|---|---|---|---|---|---|
| | Tianxia | China Chengxin | IntelliCredit | Zhima | Tencent | JD Finance | Qianhai | Koala | China Youth |
| Info specification for sharing | U | U | U | U | U | Y | U | Y | U |
| Consent requirement | Y | U | U | Y | Y | Y | Y | Y | Y |

**Table 3.** Annotation results: Third party sharing. "Y" for "Yes": the policy states explicitly which type of information is going to be shared; or the policy states explicitly that the company will require the user's consent.

## 5.4 Special purposes for data collection, usage, sharing and disclosure

As discussed in Section 5.3, companies collect, use, share and disclose personal information mainly for the purposes of providing products and services and protecting personal information. It is also common to do this for the purposes of marketing and advertising. In addition, companies include some other purposes (referred to as "special purposes" in this paper) for data collection, usage, sharing or disclosure in privacy policies. We identified six types of special purposes (see Table 4). For all the special purposes, companies usually do not need to be authorized by the user according to their own privacy policy or terms of service documents.

The most commonly quoted special purpose is "required by regulations, rules and laws, or by government organizations" indicating that compliance with legal and administrative requirements is of particular importance to the companies. In addition, "public security, public health, vital public interests" and "safeguarding the life, properties and other material interest" are also included in privacy policies across different types of companies. In most cases, special purposes are stated

| | Traditional companies | | | Internet and financial giants | | | | Others | |
|---|---|---|---|---|---|---|---|---|---|
| | Tianxia | China Chengxin | IntelliCredit | Zhima | Tencent | JD Finance | Qianhai | Koala | China Youth |
| Data collection | U | U | U | 2,4,5 | U | 1,2,3,4,6 | U | 2,4,5,6 | U |
| Data usage | 5,6 | U | U | 2,4,5 | U | 1,2,3,4,6 | 5 | 2,4,5,6 | U |
| Data sharing | 1,2,3,4 | U | U | U | 6 | 2,4,5,6 | U | 1,2,4,5,6 | U |
| Data disclosure | U | 2,5 | 5 | 2,4,5 | 2,3,4 5 | 5 | 5 | 5 | U |

1. National security, national defence
2. Public security, public health, vital public interests
3. Crime investigation, prosecution, trial and judgment
4. Safeguarding the life, properties and other material interest
5. Required by regulations, rules and laws, or by government organizations
6. Big data analysis and academic research

**Table 4.** Annotation results: Special purposes of data collection, usage, sharing and disclosure.

for data disclosure (77.8%) and are less often cited in the context of data collection (33.3%) (see Table 4).

## 5.5 Data retention

Data retention is mentioned in all the privacy-related documents in the Chinese CCRS except the one from IntelliCredit (see Table 5). But only 3 (33.3%) companies specify explicitly how long they will retain user data which varies a lot. JD Finance will retain user's information for one month (specifically after account closure) and Koala Credit will retain data permanently unless required otherwise by law or regulation.

Zhima Credit is the only company that mentions how it deals with user's negative information records. As required by the *Regulation on the Administration of the Credit Reporting Industry*, any negative information record will be retained for five years starting from the end of the "bad" behavior and then be deleted. The other 5 companies use the ambiguous terms "in a reasonable period" or "the minimum period required by law and regulation". 4 out of 9 (44.4%) companies will delete or anonymize user's personal information after the end of the relationship with the customer (e.g., closing the user account), while 3 (33.3%) companies will continue to keep the data.

| | Traditional companies | | | Internet and financial giants | | | | Others | |
|---|---|---|---|---|---|---|---|---|---|
| | Tianxia | China Chengxin | IntelliCredit | Zhima | Tencent | JD Finance | Qianhai | Koala | China Youth |
| Period specification | U | U | U | 5y | U | 1m | U | ∞ | U |
| Solution afterwards | DA | K | U | DA | DA | DA | U | K | K |

**Table 5.** Annotation results: Data retention. "DA" for "Delete/anonymize" means that the company will delete or anonymize the data afterwards; "K" for "Keep", means that the company will continue to keep the data afterwards

## 5.6 Security

6 out of 9 (66.7%) companies provide explicit information about specific techniques and management skills that are taken to protect data (see Table 6), such as using Secure Sockets Layer or training of employees. 3 companies (China Chengxin Credit, Qianhai Credit and China Youth Credit) briefly mention that the company takes technical and management measures to protect user's data in the privacy-related documents without giving any examples or listing any specific techniques or skills. IntelliCredit does not discuss this issue at all in the privacy policy.

Less than half (44.4%) of the companies state explicitly what measures they will take in case of data leakage, damage and loss. The Internet giants pay higher attention to data security than other companies as all of them not only explain the techniques and management skills taken to protect data but also establish a disaster response mechanism. Please note that all companies likely have internal security policies with further details (see, e.g., [59]).

## 5.7 Right to correct and edit

As Table 7 shows, 6 (66.7%) companies allow users to edit their personal data and 5 (55.6%) allow users to remove data. Although not explicitly illustrated in the privacy-related documents, it can be inferred that users

| | Traditional companies | | | Internet and financial giants | | | | Others | |
|---|---|---|---|---|---|---|---|---|---|
| | Tianxia | China Chengxin | IntelliCredit | Zhima | Tencent | JD Finance | Qianhai | Koala | China Youth |
| Techniques | Y | U | U | Y | Y | Y | U | Y | U |
| Management skills | Y | U | U | Y | Y | Y | U | Y | U |
| Measures for data leakage, damage and loss | U | U | U | Y | Y | Y | U | Y | U |

**Table 6.** Annotation results: Security. "Y" for "Yes", means that the policy states explicitly the techniques or management skills to protect user's data, or measures that will be taken in case of data leakage, damage or loss.

are not allowed to edit or remove their negative records. Otherwise, the credit report and scores would be of little use. But users have the right to dispute any inaccuracies about their personal information including negative records according to privacy-related documents from 6 companies, which complies with the *Regulation on the Administration of the Credit Reporting Industry*. JD Finance is the only one that specifically lists which types of personal information are allowed to be accessed, edited and removed.

When the right to edit, remove, dispute and correct is mentioned, the privacy-related documents state the ways that users can edit, remove or dispute their personal information, such as self-editing online and contacting the call center. This right is not mentioned in the privacy-related documents of IntelliCredit and China Youth Credit. We find that Tianxia Xinyong and the internet and financial giants provide more information in their privacy policies about these rights.

| | Traditional companies | | | Internet and financial giants | | | | Others | |
|---|---|---|---|---|---|---|---|---|---|
| | Tianxia | China Chengxin | IntelliCredit | Zhima | Tencent | JD Finance | Qianhai | Koala | China Youth |
| Editing | Y | U | U | Y | Y | Y | Y | Y | U |
| Removal | Y | U | U | U | Y | Y | Y | Y | U |
| Dispute/correct | Y | Y | U | Y | Y | Y | Y | U | U |

**Table 7.** Annotation results: Rights to edit and correct. "Y" for "Yes": the policy states explicitly that the user has the right to edit, remove or dispute/correct data.

## 5.8 Children and international users as specific audiences

China's first regulation on the protection of children's personal information - *Regulations on Network Protection of Children's Personal Information* took effect on October 1, 2019. The regulation sets high-level requirements for data collection, storage, use, transfer/sharing, and disclosure of children's (under 14) personal information. The *Personal Information Security Specification* also includes requirements to protect children with a distinction between minors under 14 and those above 14. Getting consent of the guardian before data collection is highlighted in both of the documents.

All internet and financial giants and 1 traditional company (55.6%) state children as a special audience and have special policy terms regarding them in the privacy-related documents (see Table 8). JD Finance requires prior consent of parents or guardians only for minors under 14 and does not include a special policy for minors above 14. Qianhai Credit has a stricter protection policy for minors as it requires consent in writing from parents or guardians before providing services to users under 18. Tencent, even though it provides products and services specifically designed for minors under 14, only requires the minors under 18 to get consent from their parents or guardians prior to using the service. Zhima Credit and Tianxia Credit use the term "minors" and do not specify any age. Also, the privacy policy of Tianxia Credit "suggests" users under 18 to seek consent and guidance from parents or guardians before information submission. China Youth Credit briefly requires that individual users must have reached 16 years of age but does not include a separate section of the information protection for children.

Although some of the 9 companies run business globally such as Alibaba and Tencent, none of them discuss privacy issues for other regions beyond mainland China in the Chinese version of the privacy policy. We merely observed that on the landing page of the app Alipay which contains Zhima Credit, the *EU General Data Protection Regulation* is listed.

| | Traditional companies | | | Internet and financial giants | | | | Others | |
|---|---|---|---|---|---|---|---|---|---|
| | Tianxia | China Chengxin | IntelliCredit | Zhima | Tencent | JD Finance | Qianhai | Koala | China Youth |
| Children | Y | U | U | Y | Y | Y | Y | U | U |
| Specific regions | U | U | U | U | U | U | U | U | U |

**Table 8.** Annotation results: Specific audience. "Y" for "Yes", means that the policy states explicitly privacy issues for children.

| | Traditional companies | | | Internet and financial giants | | | | Others | |
|---|---|---|---|---|---|---|---|---|---|
| | Tianxia | China Chengxin | IntelliCredit | Zhima | Tencent | JD Finance | Qianhai | Koala | China Youth |
| Notification | Y | Y | U | Y | Y | Y | Y | Y | Y |
| New authorisation | U | U | U | U | U | Y | U | Y | U |

**Table 9.** Annotation results: Policy change. "Y" for "Yes": the policy states explicitly that the company will notify the user or require new authorization from the user if it changes the privacy policy; "N" for "No": the policy states explicitly that the company will not notify the user or requires new authorization from the user if it changes the privacy policy.

## 5.9 Policy change

The *Personal Information Security Specification* specifies that companies have the obligation to notify the user when there is a change in the privacy policy, but does not define the methods of notification. 8 out of 9 companies (88.9%) state that they will notify users when there is a change in the privacy policy except IntelliCredit which does not mention this issue (see Table 9). The notification can either be given through posting changes on the website of the company (general notice) or through email and text message (personal notice). China Chengxin Credit, Tencent Credit, JD Finance and Koala Credit might give not only general notice but also personal notice when there is a significant change. Tianxia Xinyong and China Youth Credit, on the other hand, state explicitly that they will not send a specific notification in the above mentioned situation.

# 6 Analysis

## 6.1 Understanding the privacy practices of the Chinese CCRS with a benchmark

A brief comparison of the Chinese CCRS to credit bureaus in the U.S., which is the most discussed model in the research literature, can provide a benchmark for a better understanding of the privacy practices of the CCRS in China. We examined privacy practices of Equifax, Experian and TransUnion which are referred to as the Top 3 credit bureaus in the U.S., and found differences between them and the Chinese companies' privacy policies considering five perspectives.

First, the accessibility of privacy policies is much lower for the Chinese consumer credit reporting companies than the U.S. companies. We managed to find merely 7 privacy policies and 2 terms of service documents across 13 companies (see Section 5.1).

Secondly, the scope of data collection is similar for Chinese and U.S. consumer credit reporting companies. However, we want to highlight two aspects. On the one hand, all Chinese companies fail to present in the privacy-related documents from whom they collect different types of personal information and why they collect it, while this is clearly stated by the U.S. credit bureaus. On the other hand, collection of publicly disclosed information such as blacklists and redlists suggests one possible way how the government-run SCS and the CCRS are intertwined and is thus supposed to be a special characteristic of the Chinese CCRS. In fact, however, U.S. credit bureaus may also collect information about legal proceedings in court records (e.g., Equifax).

Thirdly, only 2 out of the 13 Chinese companies list examples of information that will be shared with third-party companies while the U.S. credit bureaus provide in detail what is going to be shared and with which companies. Fourthly, information related to data retention is listed for 7 out of the 13 Chinese companies but is not mentioned in any of the privacy policies from the 3 U.S. credit bureaus. Finally, Chinese consumer credit reporting companies provide more details on security issues such as how to deal with data leakage, damage and loss than the U.S. credit bureaus which include only very brief statements about security.

Overall, the analysis of the privacy policies suggests that the U.S. credit bureaus provide more detailed information than their Chinese counterparts regarding their privacy practices. It is important to understand the difference by taking into account the different credit reporting ecosystems in the two countries. Fundamentally, the U.S. has a more sophisticated legal system in the area of privacy protection than China, which is evidenced by the fact that both the national government and all the fifty state governments have passed privacy laws [50]. For example, the California Consumer Privacy Act which is mentioned in all the 3 U.S. credit bureaus' privacy policies pushes the companies to provide more information about data collection, sharing and usage. In China, as discussed in Section 5, there are only a few laws and regulations addressing data privacy protection; some were proposed and issued only in recent years. Nonetheless, some companies' practices in terms of privacy protection, given the privacy-related documents in our sample, appear to be in violation of the recently emerging regulations and laws, indicating the deficiency of privacy protection in China's CCRS.

The urgent problem of privacy protection in China's CCRS is further highlighted by recent data scandals and breaches involving Koala Credit. In November 2019, Koala Credit was trapped in a regulatory storm, being suspected of illegally providing personal information for nearly 100 million times [41].

## 6.2 Explaining privacy policy differences

Our annotation results reveal some differences between the three types of consumer credit reporting companies in terms of stated privacy practices. In general, privacy policies from internet giants cover a wider range of privacy issues, provide more details regarding different perspectives of data protection, and appear to be in better compliance with the regulation of privacy protection.

Here, we provide two possible explanations for the difference. First, the rapid development of big data and advanced information technology has further raised people's concerns about privacy. This is also true in China where the modern concept of privacy started to form only after the "reform and opening up" in late 1979 when China became more open to Western countries [9]. In China, people's privacy awareness and concerns are tied, to a large extent, to online services which are provided directly to individual users [37]. In other words, the public pays more attention to data privacy in the context of online services than other fields. In this situation, online service providers, in particular the internet giants, have to pay more attention to how they communicate about privacy compared to companies from other fields in China. One recent example to illustrate this: At the very beginning of 2018, when users of Alipay reviewed their annual reports of how they used the app over the past year, there was a default setting presented hardly visible on the landing page engaging users to let Alipay access their credit scores generated by Zhima Credit [11]. Both Alipay and Zhima Credit are operated by the Alibaba affiliate Ant Financial. Being seriously questioned and accused of misleading users into disclosing private information, Alipay had to remove the default setting and offer a manual option for opt-in. This public event triggered a broad and fierce discussion about privacy in China.

Second, the internet giants' global operation experience could be helpful in developing a more comprehensive privacy policy. All the 3 internet giants discussed in this paper are multinational entities. They have to follow local laws and regulations when they run business overseas. Thereby, they have accumulated more knowledge about privacy practices from regions such as the EU with advanced and comprehensive privacy regulations, which may also translate to different behavior in the domestic market. For example, as previously mentioned, Zhima Credit mentions the EU GDPR on the landing page of its app.

## 6.3 A "voluntary" CCRS

Different from the government-run SCS which is mandatory for all Chinese entities and even foreign ones who have activities in China, the commercial arm of the SCS (i.e. CCRS) is implemented on a "voluntary" basis as users have the right to opt-out of receiving the credit reporting related services such as being scored [31]. However, it remains unclear to what extent the participation in the Chinese CCRS is or can be truly *voluntary*.

Companies develop the privacy policy with non-negotiable terms and conditions. According to the annotation result (Section 5.7), individuals have the right to edit, remove, and correct/dispute about their personal data, and also to opt out of receiving emails for marketing and advertisement (at least for some CCRS companies). But they cannot change any parts of the privacy policies based on what they want, or take influence during the development of privacy policies.

Our analysis of the CCRS development shows that "social network" or "social connection" is taken as one of the credit score calculation dimensions by 7 companies (see Tables 1, 11 and 12). According to our annotation results (see Table 2), nearly half of the companies analyzed collect information of personal contacts. Taking these together, we can infer that an individual's credit score is not only based on his or her own background and activities, but also on others' behaviors and qualifications. Such data interdependence significantly weakens any voluntary character of the CCRS. Individuals who refuse to be scored but are related to those that receive credit reporting services in various ways, such as friends and family members are, to certain extent, also included in the CCRS. This leads to concerns about privacy interdependence as the protection of an individual's privacy is increasingly dependent on the actions of others and out of his or her own control [7, 48].

In addition, we found that credit scores provided by the Chinese consumer credit reporting companies can be used in a wide variety of contexts (see Tables 1, 11 and 12), which raises the question about the implications of choosing not to participate. The CCRS in Western countries concentrates on financial services, primarily assisting creditors in evaluating the credit qualities of individuals [4]. For the Chinese CCRS, however, public service turns out to be another major area for the application of credit scores. This is especially the case for credit services from the internet giants (see Section 4.2). In this case, individuals who do not use Zhima Credit may become excluded, at least partly or in certain ways, from public services such as library service or even medical treatment.

As an individual, one is left with only one convenient option: to accept the company's privacy policy and terms of service resulting in likely data transfer to receive the service. Similar to large communication platforms and social networks, it is becoming more and more difficult to reject the offers of the CCRS as the companies permeate almost every area of daily life. That means, it also becomes increasingly challenging to exclude certain data from the government-run SCS.

## 6.4 Systematic government access to private-sector data in CCRS

Previous research has observed a global trend of increasing data collection by governments and also expanding systematic government access to private-sector data [10]. The journal *International Data Privacy Law* devoted a single issue to discuss this trend in 2012. What we have learned from the CCRS indicates that China, if it does not go even further, is at least in line with other countries in pushing this trend forward.

It becomes common nowadays that high-tech companies are routinely coerced into data sharing by state institutions for security and political purposes [52, 57]. Our annotation results from the privacy polices in Section 5.4 reveal that all analyzed companies share or disclose data for purposes other than providing services and marketing. Rather, compliance with legal, judicial and administrative requirements and maintaining state security, national defense security, public security and public health, etc. are commonly quoted special purposes, implying a direct data flow from the commercial companies to the government. Especially, no explicit authorization from the user will be required in these circumstances. This echos what Abraham and Hickok termed – "A growing global trend ... is systematic governmental access, disclosure, retention, and collection of information for the purposes of surveillance, national security, and crime detection" [2].

More broadly, as discussed in Section 1, the Chinese CCRS is expected not only to fill the gap existing due to the absence of a well-developed credit reporting system in China but also to support the implementation of the SCS. The intertwined relationship between the CCRS and the SCS is highlighted in at least two ways. First, the CCRS extends the public access to the SCS based on the companies' massive client populations. Second, consumer credit reporting companies or their shareholders are actively involved in the infrastructure construction of the SCS. For example, Ant Financial, the parent company of Zhima Credit, has signed the *Memorandum on Cooperation for the Implementation of Joint Incentives and Punishment* with the National Development and Reform Commission (NDRC) [43]. As such, commercial companies make their riches of consumer data increasingly part of the overall SCS architecture.

Government's access to private-sector databases is considered as a serious risk to privacy in the U.S. [26]. Institutionally, U.S. privacy law covers not only the private sector but also the government. In contrast, existing laws and regulations about privacy protection in China target entities other than the government. Rather, there are laws and regulations granting the Chinese government extensive power of access to various databases [58]. The Chinese might have less concerns. According to the Edelman Trust Barometer, the Chinese have the highest trust in the government [19], which however also reinforces the disadvantageous position of individuals in the critical area of privacy.

# 7 Discussion & Concluding Remarks

This paper constitutes one of the first studies that investigate the development of the CCRS and privacy protection in the credit reporting domain in the context of the Chinese SCS from an empirical perspective. To be more specific, we examined 13 consumer credit reporting companies from different perspectives and analyzed in detail all privacy-related consumer-oriented documents, which we could locate.

A major concern arising from our findings is related to a power shift. In the era of big data, it is said that "data is power". As has been pointed out by previous researchers, big data is leading to a power shift between individuals and data controllers [49, 56]. Our analysis suggests that commercial companies accumulate a large amount of detailed personal information for their own credit reporting services and also support the government in big data collection, management and analysis. What is more, as the Chinese CCRS is planned and implemented within the framework of the SCS, this top-layer design consolidates the alliance between companies and the government. The "corporate-state nexus" leads to a "sovereign power" [65], resulting in big power shift between individuals, companies and the government.

The way that consumer credit reporting companies and the Chinese government cooperate under the SCS framework of the most recent corona virus crisis provides further evidence of a strong alliance between big businesses and the government and the associated power shift. In the corona virus crisis, on the one hand, an individual who is hiding any history with the novel corona virus is included in the blacklist issued by the government-run SCS in some cities such as Shanghai. On the other hand, commercial companies assigned colored QR codes to residents in more than 100 cities across China to rate people's health condition and determine whether they have to be quarantined: green codes mean free movement, yellow and red codes mean quarantine at home and supervised quarantine, respectively [54, 61]. Both Ant Financial and Tencent which are parent companies for Zhima Credit and Tencent Credit were involved in developing the health code system under the guidance of the E-government Office of the General Office of the State Council [61]. As the worst of the epidemic has passed, however, many cities started looking for new uses of the health code, indicating that such apps may outlast the outbreak. For instance, Hangzhou is exploring the use of the health code to rank or rate citizens with a "personal health index" based on their health care records, life styles, etc. [27, 64].

As the example of the health code system indicates, the "corporate-state nexus" formulated in the SCS not only enables data flow from the private sector to the government, but also fosters companies' direct participation in social control. The involvement of the private sector in the construction and implementation of the SCS complicates the process of state surveillance in China as the commercial sector has been involved in the surveillance system for the first time in a significant fashion [34]. It also further shifts power away from individuals, and pushes the surveillance economy to evolve from "enforcement" to "temptation and seduction" [6] by offering "voluntary" credit services that are heavily entangled with the government-run SCS.

In the next step, we suggest building an automated privacy-awareness enhancing system like *Polisis* for Chinese websites. Privacy policies are usually long, difficult to comprehend and evolve over time, which discourages users to engage in reading and understanding companies' data collection and data sharing practices [55]. Developing such a platform with a privacy-centric language model as the core for the Chinese websites would help to tackle these obstacles[7].

In addition, while we discussed how China's approach to regulate the CCRS is different from that in the U.S., a comprehensive and systematic comparison between the Chinese CCRS and the credit systems in other countries is warranted for further research. Our work forms a basis for such novel and extensive comparative work between regulatory regimes.

# Acknowledgments

We appreciate the detailed comments of the anonymous reviewers. We further thank Severin Engelmann, Doris Fischer, Theresa Krause, and Omar Ramon Serrano Oswald for their feedback. Mo Chen thanks for the support through a postdoc research stipend of the Fritz Thyssen Foundation. We further gratefully acknowledge funding support from the Bavarian Research Institute for Digital Transformation (bidt). Responsibility for the contents of this publication rests with the authors.

[7] Just before our submission of the camera-ready version of the paper in early June 2020, we noticed that China's parliament is poised to enact its first civil code which among other provisions protects personal information. The construction of a privacy-awareness platform would be in urgent need in this situation.

# References

[1] 01caijing, The old-brand credit reporting entity: Claimed to have data covering 1.3 billion people which was more than that in the Credit Reference Center PBoC, available at https://www.01caijing.com/article/4988.htm, August 5, 2016. Last accessed on June 9, 2020. (in Chinese)

[2] S. Abraham, and E. Hickok, Government access to private-sector data in India, *International Data Privacy Law*, 2(4): 302–315, 2012.

[3] Alibaba Group, Alibaba group published a seasonal report till the end of June 2019, available at: https://www.alibabagroup.com/cn/news/article?news=p190815, August 15, 2019. Last accessed on March 3, 2020. (in Chinese)

[4] R. B. Avery, P. S. Calem, and G. B. Canner, An overview of consumer data and credit reporting, *Federal Reserve Bulletin*, 89(2): 47-73, 2003.

[5] K. S. Ball and D. M. Wood, Political economies of surveillance, *Surveillance & Society*, 11(1/2): 1-3, 2013.

[6] Z. Bauman and D. Lyon, *Liquid Surveillance*, Cambridge: Polity, 2013.

[7] G. Biczok and P. H. Chia, Interdependent privacy: Let me share your data, *International Conference on Financial Cryptography and Data Security*, Berlin, Heidelberg, 2013.

[8] R. Botsman, Big data meets big brother as China moves to rate its citizens, *Wired*, available at: https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion, October 21, 2017. Last accessed on March 12, 2020.

[9] J. Cao, Protecting the right to privacy in China, *Victoria University of Wellington Law Review*, 36(3): 645–664, 2005.

[10] F. H. Cate, J. X. Dempsey, and I.S. Rubinstein, Systematic government access to private-sector data, *International Data Privacy Law*, 2(4): 195–199, 2012.

[11] Y. Chen, Zhima Credit admitted that using the default option of opting in to Zhima Credit in Alipay's annual bill was wrong, *The Paper*, available at: https://www.thepaper.cn/newsDetail_forward_1934070, January 4, 2018. Last accessed on June 12, 2020. (in Chinese)

[12] Y. Chen, Zhima Credit: Not thinking about making profits in two to three years, no data exchange with Baihang Credit, *The Paper*, available at: https://www.thepaper.cn/newsDetail_forward_4827406, October 31, 2019. Last accessed on March 3, 2020. (in Chinese)

[13] Y. Chen and A. Cheung, The transparent self under big data profiling: Privacy and Chinese legislation on the social credit system, *The Journal of Comparative Law*, 12(2): 356–378, 2017.

[14] China Internet Network Information Center (CCNIC), *The 45th China Statistical Report on Internet Development*, April 2020. (in Chinese)

[15] M. Chorzempa, P. Triolo, S. Sacks, China's social credit system: A mark of progress or a threat to privacy?, *Policy Briefs PB18-14, Peterson Institute for International Economics*, 2018.

[16] Credit Reference Center, *An Operation Report of Credit System Construction (2004-2014)*, The People's Bank of China, 2015. (in Chinese)

[17] R. Creemers, China's social credit system: An evolving practice of control, available at: SSRN 3175792, 2018.

[18] X. Dai, Toward a reputation state: The social credit system project of China, available at: SSRN 3193577, 2018.

[19] Edelman Trust Barometer, *2018 Edelman Trust Barometer Global Report*, 2018.

[20] S. Engelmann, M. Chen, F. Fischer, C. Kao, J. Grossklags, Clear sanctions, vague rewards: How China's social credit system currently defines good and bad Behavior, *Proceedings of the ACM Conference on Fairness, Accountability, and Transparency*, 2019.

[21] General Administration of Quality Supervision, Inspection and Quarantine and Standardization Administration, The standardization administration of China, *Information Technology Personal Information Security Specification*, GB/T 35273-2017, 2017. (in Chinese)

[22] H. Harkous, K. Fawaz, R. Lebret, F. Schaub, K. Shin, and K. Aberer, Polisis: Automated analysis and presentation of privacy policies using deep learning, *Proceedings of the 27th USENIX Security Symposium*, 2018.

[23] D. He, Y. Zhang, L. Zhang, D. Zhang, An industry report of Chinese consumer credit system, The Boston Consulting Group, 2016. (in Chinese)

[24] R. Hillman, Consumer credit: Limited information exists on extent of credit report errors and their implications for consumers, Statement for the Record Before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, 2003.

[25] S. Hoffman, Programming China: The Communist Party's autonomic approach to managing state security. *Merics China Monitor*, 44: 1-12, 2017.

[26] C. Hoofnagle, Big brother's little helpers: How ChoicePoint and other commercial data brokers collect and package your data for law enforcement, *North Carolina Journal of International Law and Commercial Regulation*, 29(4): 595–637, 2003.

[27] J. Horwitz and B. Goh, As Chinese authorities expand use of health tracking apps, privacy concerns grow, *Reuters*, available at: https://www.reuters.com/article/us-health-coronavirus-china-tech/as-chinese-authorities-expand-use-of-health-tracking-apps-privacy-concerns-grow-idUSKBN23212V, May 26, 2020. Last accessed on June 9, 2020.

[28] Z. Huang, Y. Lei, S. Shen, China's personal credit reporting system in the internet finance era: Challenges and opportunities, *China Economic Journal*, 9(3): 288–303, 2016.

[29] N. Jentzsch, The economics and regulation of financial privacy: An international comparison of credit reporting systems, *Springer Science & Business Media*, 2006.

[30] N. Jentzsch, An economic analysis of China's credit information monopoly, *China Economic Review*, 19(4): 537–550, 2008.

[31] G. Kostka, China's social credit systems and public opinion: Explaining high levels of approval, *New Media & Society*, 21(7): 1565–1593, 2019.

[32] L. Kuo, China bans 23m from buying travel tickets as part of 'social credit' system, *The Guardian*, available at: https://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system, March 1, 2019. Last accessed on March 14, 2020.

[33] X. Li, Building "Credit China" from a window, *China Daily*, available at: http://finance.people.com.cn/n/2015/0720/c1004-27327526.html, July 20, 2015. Last accessed on June 7, 2020. (in Chinese)

[34] F. Liang, V. Das, N. Kostyuk, and Hussain, M. M. Constructing a datadriven society: China's social credit system as a state surveillance infrastructure, *Policy & Internet*, 10(4): 415-453, 2018.

[35] J. Lin, Lin Junyue: Why it is said that the construction of the social credit system started in 1999?, available at: https://m.credit100.com/xhxy/c/2019-09-09/535610.shtml, September 9, 2019. Last accessed on March 12, 2020. (in Chinese)

[36] C. Liu, Multiple social credit systems in China, *Economic Sociology: The European Electronic Newsletter*, 21(1): 22-32, 2019.

[37] Y. Lv, Privacy and data privacy issus in contemporary China, *Ethics and Information Technology*, 7: 7-15, 2005.

[38] D. Marron, *Consumer credit in the United States: A sociological perspective from the 19th century to the present*, New York, NY: Palgrave Macmillan, 2016.

[39] M. Meissner, R. Creemers, P. K. Crossley, P. Mattis, and S. Hoffman, Is big data increasing Beijing's capacity for control?, available at: http://www.chinafile.com/conversation/Is-Big-Data-Increasing-Beijing-Capacity-Control, August 10, 2016. Last accessed on March 12, 2020.

[40] M. Meissner, and J. Wübbeke, In: S. Heilmann, M. Stepan (Ed.), *China's Core Executive Leadership Styles, Structures and Processes under Xi Jinping* (Merics 2016) 52.

[41] F. Meng and Y. Song, Koala Credit is suspected of leaking billions of citizens' personal data, *Beijing Business Today*, reproduced by *people.cn* at http://capital.people.com.cn/BIG5/n1/2019/1121/c405954-31466186.html, November 21, 2019. (in Chinese) Last accessed on May 24, 2020. (in Chinese)

[42] S. Mistreanu, Life inside China's social credit laboratory: The party's massive experiment in ranking and monitoring Chinese citizens has already started, *Foreign Policy*, available at: https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/, April 3, 2018. Last accessed on March 12, 2020.

[43] National Development and Reform Commission (NDRC), National Development and Reform Commission and Ant Financial signed a Memorandum on Cooperation for the Implementation of Joint Incentive and Punishment, available at NDRC's website https://www.ndrc.gov.cn/fzggw/jgsj/cjd/sjdt/201608/t20160803_1111383.html, August 3, 2016. Last accessed on March 4, 2020. (in Chinese)

[44] M. Ohlberg, S. Ahmed, B. Lang, Central planning, local experiments: The complex implementation of China's social credit system, Merics, 2018.

[45] R. Olegario, *The Engine of Enterprise: Credit in America*, MA: Harvard University Press, 2016.

[46] B. Patru, How China's social credit system will erode privacy in the West, *CPO Magazine*, available at: https://www.cpomagazine.com/cyber-security/how-chinas-social-credit-system-will-erode-privacy-in-the-west/, 2019. Last accessed on March 14, 2020.

[47] M. Persson, M. Vlaskamp and F. Obbema, China rates its own citizens Including online behavior, available at: https://www.volkskrant.nl/nieuws-achtergrond/china-rates-its-own-citizens-including-online-behaviour~b4c0ae0e/, 2015. Last accessed on January 16, 2020.

[48] Y. Pu, and J. Grossklags, Towards a model on the factors influencing social app users' valuation of interdependent privacy, *Proceedings on Privacy Enhancing Technologies*, 2016(2): 61-81, 2016.

[49] M. Rhoen, Beyond consent: Improving data protection through consumer protection law, *Internet Policy Review*, 5(1): 1-15, 2016.

[50] N. M. Richards, A. B. Serwin, and T. Blake, Understanding American privacy, in G. González Fuster, R. van Brakel and P. De Hert (eds.), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics*, Edward Elgar Publishing, 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256918.

[51] A. Schmitz, Secret consumer scores and segmentations: Separating haves from have-nots, *Michigan State Law Review*, 2014(5): 1411–1473, 2014.

[52] S. Shorey and P. Howard, Automation, big data, and politics: A research review, *International Journal of Communication*, 10: 5032-5055, 2016.

[53] State Council, *Planning Outline for the Construction of a Social Credit System (2014-2020)*, June 2014. (in Chinese)

[54] Tencent Tech, Tencent health code is used by 1.6 billion people, available at: https://tech.qq.com/a/20200310/016327.htm, March 10, 2020. Last visited on March 11, 2020. (in Chinese)

[55] J. Turow, C. Hoofnagle, D. Mulligan, N. Good and J. Grossklags, The Federal Trade Commission and Consumer Privacy in the Coming Decade, *I/S: A Journal of Law and Policy for the Information Society*, 3(3): 723-749, 2008.

[56] L. Ulbricht and M. von Grafenstein, Big data: Big power shift?, *Internet Policy Review*, 5(1): 1-15, 2016.

[57] J. Van Dijck, Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology, *Surveillance & Society*, 12(2): 197-208, 2014.

[58] Z. Wang, Systematic government access to private-sector data in China, *International Data Privacy Law*, 2(4), 220–229, 2012.

[59] J. Weidman and J. Grossklags, What's in Your Policy: An Analysis of the Current State of Information Security Policies in Academic Institutions, *Proceedings of the 26th European Conference on Information Systems (ECIS)*, 2018.

[60] Xinhua, The People's Bank of China: The credit reference system has covered 990 million individuals, available at: http://www.xinhuanet.com/2019-06/15/c_1124626094.htm, June 15, 2019. Last accessed on June 15, 2020. (in Chinese)

[61] Xinhua, Alipay health code was implemented in over 100 cities in 7 days; the digitalisation of epidemic prevention is characterised by "China Speed", available at: http://www.xinhuanet.com/tech/2020-02/19/c_1125596647.htm, February 19, 2020. Last accessed on March 11, 2020. (in Chinese)

[62] Y. Xu, None of the eight companies was qualified for the license for running consumer credit reporting business after the two-years experiment, *Yicai*, available at: https://www.yicai.com/news/5271750.html, April 23, 2017. Last accessed on June 10, 2020. (in Chinese)

[63] Z. Zhang, Institutional Construction for social credit system in the era of big data, *Credit Reference*, 9(212), 58-61, 2016.

[64] R. Zhong, China's virus apps may outlast the outbreak, stirring privacy fears, *The New York Times*, available at: creditchina.gov.cn/gerenxinyong/?navPage=14, May 26, 2020. Last accessed on June 9, 2020.

[65] S. Zuboff, Big other: Surveillance capitalism and the prospects of an information civillization, *Journal of Information Technology*, 30(1), 75-89, 2015.

# Appendix

There are four tables in the Appendix (Table 10 to Table 13). Table 10 presents a comparison of instrument categories used by *Polisis* and the current research; Table 11 and Table 12 are about characteristics of internet and financial giants, and other consumer credit reporting companies, respectively; Table 13 gives an example of our coding of the privacy-related documents.

| **Polisis** | **Current Research** |
|---|---|
| Data collection | Data collection (personal sensitive information; other information) |
| Third party sharing | Third-party sharing |
| Security | Security |
| Data retention | Data retention |
| Specific audiences | Specific audiences |
| Policy change | Policy change |
| Rights to edit | Rights to edit and correct |
| Your choice | Special purposes of data collection, usage and sharing |

**Table 10.** A comparison of instrument categories used by *Polisis* and the current research

| Consumer Credit Score | Companies | Stakeholders | Data Resources | Calculation Dimensions | Algorithms | Application Areas |
|---|---|---|---|---|---|---|
| **Zhima Credit Score/芝麻分 (350-950)** | Ant Financial (蚂蚁金服) | Alibaba | Alibaba e-commerce platform; Ant Financial; Information uploaded by users; Business partners; Financial institutions and public institutions | 1. Credit history; 2. Behavioral preference; 3. Contractual capacity; 4. Identity qualities; 5. Social network | Machine learning and cloud computing | Finance; Public service; E-commerce |
| **Tencent Credit Score/腾讯信用分 (300-850)** | Tencent Credit (腾讯征信) | Tencent Group | Social network platforms (QQ and Wechat); Tenpay transactions; Entertainment (online game); Information uploaded by users; Partners | 1. Contractual capacity; 2. Security; 3. Fortune; 4. Consumption; 5. Social network | Use of TD-BANK, methods of statistics and traditional machine learning | Finance |
| **Xiaobai Credit Score/小白信用分 (0-110)** | JD Finance (京东金融) | JD.com | JD.com e-commerce platform, JD Finance | 1. Identity information; 2. Contractual capacity; 3. Assets; 4. Online consumption preference; 5. Social network | Big data algorithms | E-commerce; Finance; Public service; Job hunting |
| **Panshi Xiaomanfen/磐石小满分* (350-950)** | Du Xiaoman Financial (度小满金融) | Baidu | N.A. | 1. Credit history; 2. Contractual capacity; 3. Identity qualities | Big data, AI | Finance (mainly about service from Du Xiaoman Financial); Marketing |
| **Credoo Score/好信分 (300-850)** | Qianhai Credit (前海征信) | Ping An Insurance | Ping An Insurance; Public institutions; Business partners | 1. Identity info; 2. Contractual capacity; 3. Risk of dishonest behavior; 4. Consumption preference; 5. Behavioral characteristics; 6. Social network credit; 7. Growth potential | Multidimensional nano modelling | Finance; E-commerce; Public good |

**Table 11.** Internet and Financial Giants. Similar to the data source provided in Figure 1, the shareholder information is from the company's website and Tianyancha (https://www.tianyancha.com/). Information for data resource, algorithms, calculation dimensions and application areas is based on the companyies' websites, a BCG report [23], and Chinese official media press "people.cn"(http://history.people.com.cn/peoplevision/n/2015/0731/c371452-27391634.html. For JD Finance, also refer to *Xinhua News* (http://www.xinhuanet.com/tech/2019-08/21/c_1124903088.htm) and *Fortune World* (http://www.fortuneworld.com.cn/internet/201801/t20180111_2978288.shtml). For Qianhai Credit, also refer to a report from the 01 Think Tank (https://www.01caijing.com/article/4826.htm). *Short before the submission of the paper, we learned that "Panshi Xiaomanfen" is now not available on the company's website and is replaced with "Panshi qualification indicator".

| Consumer Credit Score | Company | Stakeholders | Data Resources | Calculation Dimensions | Algorithms | Application Areas |
|---|---|---|---|---|---|---|
| **N.A.** | Baihang Credit/百行征信 | NIFA, Pengyuan Credit, China Chengxin Credit, IntelliCredit, Zhima Credit, Tencent Credit, Qianhai Credit, Koala Credit and Sinoway Credit | N.A. | N.A. | N.A. | N.A. |
| **Koala Score/考拉 分(300-850)** | Koala Credit/考拉信用 | Lakala Credit Management | Lakala Credit Management; Business partners; Public institutions | 1. Contractual capacity; 2. Credit history; 3. Identity qualities; 4. Transaction behavior; 5. Social network | Traditional Delphi method; Regression；Web-mining; Classification Neural networks; Big data processing and multi-perspective combo modeling | Finance; E-commerce |
| **Zhuzhu Score/猪猪分(up to 1000)** | Sinoway/华道征信 | Four large companies | Stakeholders' database; Business partners; Public institutions | 1. Identity authentication; 2. Background qualities; 3. Living credit; 4. Consumption level; 5. Daily activities | N.A. | Finance; Apartment rental; Human resource; Marriage market |
| **Uniscore/优你 分(350-800)** | China Youth Credit/中青信用 | Tsinghua Unigroup | National and local governments; Public institutions; Business partners | 1. Personal information; 2. Volunteer work; 3. Social connections; 4. Credit history; 5. Consumption history; 6. Track record of honouring contracts | Big data and cloud computing technology; Evaluation model; Financial risk control | Human resource; Studying abroad; E-commerce; Finance |
| **N.A.** | Wanda Credit/万达征信 | Wanda Group | Wanda Group (retail data; Feifan Business Coalition); Business partners | N.A. | Big data mining and analytics | N.A. |

**Table 12.** Other Consumer Credit Reporting Companies. Similar to the data source provided in Figure 1, the shareholder information is from the company's website and Tianyancha (https://www.tianyancha.com/). Information for data resource, algorithms, calculation dimensions and application areas is based on the companyies' websites, a BCG report [20], and Chinese official media press "people.cn" (http://history.people.com.cn/peoplevision/n/2015/0731/c371452-27391634.html). For Sinoway, also refer to *Tech.163* (http://tech.163.com/15/0601/08/AR0R93DD000915BF.html); for Koala Credit, also refer to *Paynews* (http://paynews.net/article-29207-1.html); for China Youth Credit, also refer to *South China Morning Post* (https://www.scmp.com/tech/apps-social/article/3003158/small-team-building-social-credit-system-app-chinas-youth).

| Taxonomies and Questions | Original Text | Translation |
|---|---|---|
| **Data collection** - sensitive information: Item 7-Online activities information | | |
| Yes. The policy states it explicitly. | 为了尽量科学、全面、客观、公正地向您提供信用评估及信用管理服务....我们需要收集与您信用相关的真实、准确、全面的信息，主要包括:...(2)您在使用第三方产品或服务中与您信用相关的信息。例如：您在电商网站上的交易信息、使用支付机构服务产生的支付信息，使用信用免押服务后是否按约支付了租金，在租车平台上使用租车服务后是否按约支付了服务费等。 | In order to provide you with credit evaluation and credit management services as scientifically, comprehensively, objectively, and impartially as possible ... we need to collect true, accurate, and comprehensive information related to your credit, mainly including: (2) Information related to your credit in your use of third-party products or services. For example: your transaction information on the e-commerce platform, payment information generated by the use of payment agency services, whether the rent was paid as agreed after using the deposit-free service, whether the service fee was paid as agreed after using the car rental service on the car rental platform. |
| No. The policy states explicitly that the company/institution will not do that. | 我们不会收集您的宗教信仰、基因、指纹、血型、疾病和病史信息，也不会收集您的聊天、通话内容及您在社交媒体上的言论。 | We will not collect information about your religion, genes, fingerprints, blood type, disease, and medical history, nor do we collect your chats, calls, and your speech on social media. |
| **Data collection** - other information: Item 12-Publicly disclosed information | | |
| Yes. The policy states it explicitly. | 为了尽量科学、全面、客观、公正地向您提供信用评估及信用管理服务....我们需要收集与您信用相关的真实、准确、全面的信息，主要包括:...(3)与信用相关的司法、行政信息。例如：法院依法公开披露的被执行人名单信息。(4)合法公开披露（例如合法的新闻报道、政府信息公开等渠道）的信息中或您自行公开的信息中与信用有关的信息。 | In order to provide you with credit evaluation and credit management services as scientifically, comprehensively, objectively, and impartially as possible ... we need to collect true, accurate, and comprehensive information related to your credit, mainly including: (3) relevant judicial and administrative information that is related to credit. For example: the list of enforced persons issued publicly by the court according to law. (4) Credit-related information in legally publicly disclosed information (such as legal news reports, government information disclosure, etc.) or information that you publicly disclose. |
| **Data Retention**: Item 19-Retention period | | |
| Yes. The policy states it explicitly. | 关闭后，您芝麻信用帐户内的信息将被清空。但请您了解，为了准确记录，维护安全的网络交易环境，我们将对您的不良信息进行妥善保存，保存期限为自不良行为或事件终止之日起5年；超过5年的，我们将依法予以删除。 | After closing (the account), the information in your Sesame Credit account will be cleared. However, please understand that in order to accurately record and maintain a secure online transaction environment, we will properly store information about your bad conduct for a period of 5 years from the date of the termination of the bad conduct or incident; when it exceeds 5 years, we will delete it according to the law. |
| Unclear | 关闭后，您芝麻信用帐户内的信息将被清空。... 我们仅在本政策所述目的所必需期间和法律法规及监管规定的时限内保存您的个人信息。 | After closing (the account), the information in your Sesame Credit account will be cleared. ... We only store your personal information for the time period that is necessary for the purposes described in this policy and for the time period required by laws and regulations. |
| **Security**: Item 23-Measures for data leakage, damage or loss | | |
| Yes. The policy states it explicitly. | 若不幸发生个人信息安全事件，我们将按照法律法规的要求，及时向您告知：安全事件的基本情况和可能的影响、我们已采取或将要采取的处置措施、您可自主防范和降低风险的建议、对您的补救措施等。我们将及时将事件相关情况以客户端推送通知、发送邮件、短消息等方式告知您，难以逐一告知用户时，我们会采取公告的方式进行告知。同时，我们还将按照监管部门要求，主动上报个人信息安全事件的处置情况。 | In the unfortunate event of a personal information security incident, we will promptly inform you in accordance with the requirements of laws and regulations: the basic situation and possible impact of the security incident, the measures we have taken or are about to take, and suggestions on how you can prevent and reduce risks on your own, and remedies, etc. We will promptly inform you of the event by pushing client notifications, sending emails, short messages, etc. If it is difficult to notify users one by one, we will use an announcement to inform all clients. At the same time, we will proactively report the handling of personal information security incidents in accordance with the requirements of regulatory authorities. |

**Table 13.** Coding sample.