Cutting-edge Insight into Field Observation
Professional Pilot of Industry Guidance

5G

APPLICATION SCENARIOS AND PRIVACY PROTECTION RESEARCH REPORT

ZTE Data Protection Compliance Dept

2020/5/25

Preface

At present, the digital economy has become the engine leading the global economic development, bringing the economic society into a new era and driving the traditional industries to develop towards digitalization, networking, and intelligence. The 5th generation mobile networks (5G) technology provides the advantages of large bandwidth, ultra-high density connection and high reliability and low latency. It improves the performance of the communication network, provides AI infrastructure platform for the Internet of Everything and Human-machine Interaction, and provides infinite space for the innovative development of digital economy.

5G technology injects brand new vitality into various typical application scenarios. The improvement of transmission rate, connection density, real-time performance and reliability brought by 5G have created new value growth points for the application scenarios derived from Mega Video, Industrial Internet, Internet of Vehicles, Telemedicine, Intelligent Security, Intelligent Campus, Intelligent Grid, Intelligent Airport, Intelligent Transportation, and Intelligent Finance.

In the Internet of Everything (IoT) era, data has become a production factor, and human-oriented products and services have become the core value center. The collection and storage of user privacy data (personal information) is under explosive growth. Individuals, enterprises, industries, and even countries are closely connected through data exchange. 5G application scenarios cover most of the hotspot areas in future social production and economic life. With the deepening of global privacy protection laws and regulations, privacy protection compliance has become an important prerequisite for the application in these fields. Complying with privacy protection requirements in the process of promoting digital economy, standardizing data sharing, facilitating application scenario innovation and accelerating 5G "new infrastructure" to ensure legitimacy and compliance has become a topic requiring close attention and research for all parties concerned.

Based on the technical features and application scenarios of 5G, this report conducts the research from the perspectives of privacy protection and data compliance. It is committed to achieving professional and industry guidance through "Cutting-edge Insight into Field Observation" helping all parties involved in the 5G industry chain understand application scenarios and privacy protection concerns, and providing reference for good compliance implementation and privacy protection design.

Editor
May 25, 2020

Table of Contents

1. Digital Economy and 5G Application Scenarios

At present, the digital economy has become the engine leading the global economic development, bringing the economic society into a new era and driving the traditional industries to develop towards digitalization, networking, and intelligence. Major countries and regions around the world have launched digital national strategies, focusing on key areas such as industries, finance, culture creativity, and artificial intelligence, in order to improve national innovation capabilities through the development of the digital economy. Digital economy uses digital knowledge and information as key production factors, modern information networks as important carriers, and information communication technologies as critical impetus for efficiency improvement and economic structure optimization.

From the 1st generation mobile networks (1G) to the 4th generation mobile networks (4G), the communication technology is designed to meet the communication requirements between individual users. In the digital transformation of industries, big data, artificial intelligence, cloud computing, Internet of Things (IoT) and other new technologies are continuously integrated and innovated, imposing more stringent requirements for communication networks. The 5G communication technology introduces network function virtualization and software-defined network technologies, and provides high bandwidth, ultra-high density connection, high reliability with low latency features. This technology achieves the tremendous performance improvement of communication networks, provides an open key infrastructure platform for the Internet of Everything and Human-machine Interaction, and provides infinite space for the innovative development of digital economy.

According to the 3rd Generation Partnership Project (3GPP) of the International Mobile Communication Standardization Organization, the 5G network defines three application scenarios of technical features: (1) Enhanced Mobile Broadband: Providing 100Mbps-1Gbps user experience rate and 100Gbps peak rate; (2) Mass Machine Communication: Supporting 1 million connections per square kilometer and longer battery life; (3) Ultra-reliable and Low-Latency Communication: Providing 1 ms latency in uu interfaces and 99.999% transmission reliability. The 5G network provides a variety of industrial application scenarios: (1) Enhanced Mobile Broadband: Mainly focusing on bandwidth-sensitive services, such as 4K/8K UHD video, Virtual Reality / Augmented Reality (VR/AR) panoramic live broadcast, VR/AR entertainment etc.; (2) Massive-machine communication: Mainly focusing on IoT services, such as Intelligent City, Intelligent Home, Intelligent Transportation, Intelligent Campus, Intelligent Airport, and Intelligent Agriculture. (3) Ultra-reliable and Low-Latency Communication: Mainly focusing on high-reliability and low-latency services, such as Industrial Internet, Internet of Vehicles Automatic Driving, and Telemedicine.

Nowadays, the standard protocols of 5G networks are gradually developing and maturing, and they can pave the way for new 5G commercial applications, meet the network requirements of various application scenarios, and facilitate the digital transformation and intelligent development of various industries.

2. Digital Economy and Privacy Protection

With the advent of the digital economy era, the integration between individuals and the digital economy is deepening, and the privacy protection problem is becoming increasingly prominent. Privacy protection laws and regulations have mushroomed around the world. Representative legislation such as the Personal Information

Protection Law (PIPL) of the People's Republic of China, the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA) in the United States, and the General Data Protection Act in Brazil (Lei Geral de Prote o de Dados Pessoais, LGPD).

Meanwhile, privacy protection standards are released intensively. For example, in August 2019, the International Organization for Standardization (ISO) and the International Electrotechnical Commission（IEC） jointly released the Personal Information Management System (PIMS) international standard ISO/IEC 27701 :2019. From 2019 to 2020, the National Standardization Administration Committee of China released GB/T 37964 -2019 Information Security Technologies, Personal Information Deidentification Guide, GB/T 35273 -2020 Information Security Technologies, Personal Information Security Specifications, GB/T 39335-2020 Information Security Technologies, Personal Information Security Impact Assessment Guide, to provide a standard guidance for privacy protection.

In the Internet of Everything era, data has become a production factor, and human-oriented products and services have become the core value center. The collection and storage of user privacy data (personal information) is under explosive growth. Individuals, enterprises, industries, and even countries are closely connected through data exchange. The high-frequency use and rapid flow of personal data in social production and life have a profound impact on the responses to the requests of data subjects rights, and bring challenges to enterprises in fulfilling their privacy protection obligations. Specifically, the widely distributed sensors with wide distribution introduce mass data; Cloud computing provides support for mass data storage and processing with the flexible allocation of resources; Big data technology is used for data processing, analytics and prediction; And artificial intelligence (AI) efficiently implements the data analytics application. The coordinated operation of these new technologies not only serves the economic and social development, but also makes privacy protection more complicated.

At present, complying with privacy protection requirements in the process of promoting digital economy, standardizing data sharing, facilitating application scenario innovation and accelerating 5G "new infrastructure" to ensure legitimacy and compliance has become a topic requiring close attention and research for all parties concerned.

3. 5G Application Scenarios and Privacy Protection

5G application scenarios cover most of the hotspot areas in future social production and economic life. With the deepening of global privacy protection laws and regulations, privacy protection compliance has become an important prerequisite for the application in these fields. For example, the pan-sensing intelligent devices supported by 5G communications technologies will be ubiquitous in production and life, collecting massive data and associating them with individuals. People's lives and work are increasingly dependent on these intelligent devices, and data collection, storage, transmission, and usage will be further enhanced. Meanwhile, data security and privacy protection have not kept up with data flow and development. In recent years, numerous and increasingly serious large-scale data breaches and personal data abuses have brought warnings to the application development and scenario embedded with 5G in various fields, which brings the self-evident importance and urgency to privacy protection compliance .

3.1. Privacy Protection Challenges in 5G Application Scenarios

The 5G era has brought new changes to technologies and application scenarios. The major challenges to privacy protection are as follows: (1) The coverage of millimeter waves and small base stations is narrowed, user positioning is more accurate, and real-time location information collection is more convenient. (2) Ubiquitous sensing equipment helps to establish wider connections between people, between people and objects and between objects. The personal data types and volumes have increased explosively. The equipment data in the traditional understanding is tagged with the personal data label after being associated with the individual. (3) The number of connected devices increases dramatically, the networking environment becomes more complicated, and the possibility of fragile devices failing also increases. (4) Data flow paths are changeable, service cooperation modes are diversified, data processing roles are numerous, and multi-management is more complicated. (5) The integration, development, and innovative applications of big data, artificial intelligence, cloud computing, IoT, and other new technologies have higher requirements for privacy protection management and technical measures.

3.2. Privacy Protection in 5G Application Scenarios

3.2.1. Internet of Vehicles (IoV)

[Application Scenario Overview]

With the improvement of vehicle intelligence, IoV has become the focus of domestic and overseas automobile enterprises. The large bandwidth and low latency of 5G are mainly used in automatic driving and vehicle road coordination. The main scenarios are as follows:

1) Vehicle Informatization Services: high-precision map during vehicle driving, traffic signal light warning, peripheral service information push.
2) Traffic Safety Applications: intelligent traffic management, and fast acquisition of safety information during vehicle driving.
3) Transportation Efficiency Applications: vehicle-road-people collaboration, road speed guidance, vehicle path optimization, and road traffic optimization.
4) Highly Collaborative Applications: vehicle team collaboration, vehicle-road collaboration, and remote scheduling in transportation or logistics industry.

[Data Processing Analysis]

The data processing in IoV involves a large number of entities and complex data types. Since it is related to traffic safety and public interest, it has become a focus of public concern. Many entities, such as automobile manufacturers, vehicle-mounted system developers, repair factories, information entertainment system providers, content providers, road infrastructure administrators, insurance companies, vehicle distributors, public management organizations, vehicle-mounted service providers and telecom operators, etc., may participate in a same data processing activity to different extent. IoV generates massive data, most of which can be regarded as personal data.

IoV mainly includes personal data types as below:

Data Categories	Data Types	Potential Data Controller / Processor
Drivers' information	Name, ID No., driver's license ID, mobile phone number, email, payment information, biometric information (such as face, voiceprint, fingerprint and heart rate), driving habits, health status,	Leasing or sharing service provider, system service provider, rescue organization, insurance company, vehicle-mounted service provider, etc.

	location information, etc.	
Vehicle-related information	Vehicle identification code (VIN), operation and control records, travel route records, vehicle configuration information, vehicle status information (such as mileage, component wear, status and charging records), real-time operation information (speed, engine speed, tire pressure, oil meter, and coolant status), repair records, insurance information, etc.	Host manufacturers, accessories manufacturers, leased or shared service providers, system service providers, rescue organizations, insurance company, system service providers, vehicle-mounted service providers, repair vendors, second-hand traders, and transportation departments, etc.
Vehicle-mounted terminal / application-related information	Various information of vehicle-mounted terminal and mobile phone, such as name, account and password, location information, payment information, play records, personal preferences, route planning, contact list, call records, etc.	Vehicle-mounted terminal system service providers, vehicle-mounted service providers, and content providers, etc.
Other information	Environment perception information (pedestrian and passing vehicles), owner information, passenger information, weather information and location information, etc.	Vehicle sellers, rescue organizations, insurance company, vehicle-mounted service providers, etc.

[Main Concerns]

Main concerns of IoV privacy protection and the corresponding scenarios are as follows：

Main concerns of privacy protection	Application Scenario	Risk Level
Comprehensive analysis of data processing relationships	Vehicle-road coordination, traffic safety management, and vehicle-mounted application services	High
Users' location information	Vehicle-road coordination, traffic safety management, and vehicle-mounted application services	High
Biometric information, such as facial recognition, voiceprint recognition, and fingerprint recognition	On-board application services	High
Biological health information	Traffic safety management, vehicle-mounted application services	High
Children data	Traffic safety management, vehicle-mounted application services	High
Accurate user profiling	Vehicle-road coordination, traffic safety management, and vehicle-mounted application services	High
Data security management	IoV related scenarios	High
Data transfer evaluation	Cross-border data transfer	High

[Related Cases]

In September 2011, the US Federal Trade Commission (FTC) investigated GM Angie Star, accusing it of tracking the driver's behaviors. After modifying the user information sharing strategy, GM Angie Star may share the vehicle location, speed and seat belt usage information with third parties or even sell the information to others, including law enforcement agencies, wireless network suppliers and data management companies. In 2011, U.S. white-cap hackers Miller and Valasek successfully hacked Toyota Prius and Ford Escape, and in 2015, they remotely controlled a Chrysler Nokie vehicle, not only controlling the facilities inside the vehicle, but also controlling the speed and route of the vehicle. A Dutch network security company announced in 2018 that some In-Vehicle Infotainment (IVI) systems have serious problems that attackers can listen to the conversation within the vehicle, remotely manipulate the microphone, access the entire address book and historical conversation records, and even precisely locate the vehicle through the inside navigation system and automatically update at any time.

3.2.2. Intellectual Campus

[Application Scenario Overview]

The main application scenarios of 5G in Intellectual Campus include cloud VR education, campus HD live broadcast, remote interactive education, and campus video monitoring. 5G is promoting the reconstruction of education services to create seamless and immersive educational experience supported by ubiquitous perception networks. Management business, teaching business, training business, and service business in the education industry will share information for data exchange. The intelligent learning service system will perform precise analysis for individuals, and provide them with high-quality resources and services in accordance with their specific requirements and characteristics, thus accelerating the construction of intellectual campuses.

[Data Processing Analysis]

In Intellectual Campus scenario, personal data is widely processed in the aspects as follows:

1) In terms of **infrastructure**, human-object-scene information in campus can be fully captured through computers, mobile phones, sensors, cameras, and wearable devices, which involves sensitive information such as personal location information and biometric information. For example, the attendance management function can manage the attendance of students, teachers, and laboratory administrators, etc. and perform route attendance management to security officers, which process personal location information.
2) In terms of **data support**, the campus basic information library, individual education library, course education library, class education management library, and school education management library can be established via analyzing the summaries of teaching regular patterns, which involves user profiling activity and personal basic education information processing.
3) In terms of **platform capabilities**, platform capability support services catered for the Intelligent Campus IoT applications can be established, including unified user authentication and open interface access capability, security authentication capability, service capability of cloud computing and storage, large data analysis and decision-making support capability, and situational perception capability, which may involve the processing of biometric data such as facial recognition.
4) In terms of **users**, intelligent support for different roles under different scenarios and terminal devices can be provided, for example, personalized learning services for students, precise teaching and research services for teachers, data-driven management services for administrators, and education governance services,which may involve sensitive data processing for individual users.

Intellectual Campus mainly includes personal data types as below:

Data Categories	Data Types	Potential Data Controller / Processor
Basic ID information	Name, ID number, campus ID, fingerprint, and facial recognition information, etc.	Government, schools, security product suppliers
Attendance information	Fingerprint and location	Government, schools, security product suppliers
Monitoring Device Information	Location and facial recognition, etc.	Schools , monitoring equipment suppliers
VR/AR equipment related information	Voiceprint and fingerprint, etc.	VR/AR equipment suppliers, wearable equipment suppliers
Distance interactive education	Account, password, and personal portrait, etc.	Schools, talent markets, operators, database suppliers, virtual website platforms, cloud storage suppliers, mega video suppliers
Related information of the Big Data platform	Personal portrait information that combines basic personal information and education resumes, classroom performance, and learning effectiveness analysis, etc.	Government, schools, talent markets, operators, database suppliers, internet virtual platforms, cloud storage suppliers

[Main Concerns]

Main concerns of privacy protection in Intellectual Campus and the corresponding scenarios are as follows:

Main concerns of privacy protection	Application Scenario	Risk Level
Personal location information	Route attendance management of security officers	Low
Biometric information, such as facial recognition, voiceprint recognition, and fingerprint recognition	Attendance management of students, teachers, and laboratory administrators.	High
User profiling	Closed-loop teaching evaluation and educational management, teaching effectiveness analysis; recommendation of academic/life/entertainment information based on personal preferences; AI robot teaching assistance and personalized teaching;	High
Monitoring	Security monitoring	High
User consent and permission setting	Cloud data processing	Medium

[Related Cases]

In November 2019, the Swedish Anderstorps High School used the facial recognition technology in a pilot project to record students' attendance in order to simplify the operation and automatically register the course. This experimental project lasted for three weeks, involving 22 students. Students' facial recognition data and full names are captured in photos and stored on local computers that are not connected to the network. Before collecting students' biometric data, the school obtained the guardian's express consent. However, the school did not conduct privacy impact assessment or negotiate with the Swedish data protection agency. The Swedish Data Protection Agency penalized the high school for the violation of GDPR.

3.2.3. Industrial Internet

[Application Scenario Overview]

The Industrial Internet is a combination of industrial technologies and information communication technologies. It integrates and upgrades Information Technology (IT), Communication Technology (CT) and Operational Technology (OT). At present, the overall digitalization and intelligence level in the industrial field is still low. The requirements of the industrial Internet include device mobility solution, device operation status data collection, remote machine control, remote intelligent monitoring, remote device maintenance, industrial flexible production, labor liberation, identification of dangerous scenarios and personal safety guarantee, in order to improve productivity and operation efficiency and reduce overall costs. To accelerate the Industrial Internet and cloudification processes to meet these requirements and application scenarios, communication networks must:

1) Achieve **continuous coverage**, to ensure security and high reliability.
2) Provide both uplink and downlink support on **high-rate data transmission**;
3) Provide **real-time control at millisecond level**; and
4) Provide support on IoT connections with **massive high concurrency** and medium/high data rate in certain areas.

The large bandwidth, low latency and wide connections of 5G network, combined with XR (VR/AR), Mobile Edge Computing (MEC), Artificial Intelligence (AI) and big data, displays features the ubiquitous perception, ubiquitous connection and ubiquitous intelligence, which can well meet the development demands of intelligent industrial networks. The 5G networks deployment in the industrial field and the combination with cloud services and MEC technologies can accelerate the transformation of intelligent industries and to facilitate the new digital applications build-up.

[Data Processing Analysis]

In the current major application scenarios of Industrial Internet, the scenarios involving personal data processing include: XR auxiliary assembly, XR auxiliary remote maintenance/monitoring, XR remote control operation, XR auxiliary training and industrial App, etc.. Examples of personal data types involved in Industrial Internet are as follows:

Data Categories	Data Types	Potential Data Controller / Processor
Personnel identity information	Personnel name, employee ID, operation account, and password, etc.	Industrial enterprises, equipment / software / cloud service providers
Operation	Biometric information (such as fingerprints, facial	Industrial enterprises, equipment /

Information	recognition, voice print, and iris) and physiological detection information (such as eyeball tracing, heart rate, and blood pressure), operation records, activity records, environmental information, and further analysis of operation information, etc.	software / cloud service providers
Training information	Training records, operation records, response information, and further analysis information, etc.	Industrial enterprises, equipment / software / cloud service providers

[Main Concerns]

Main concerns of Industrial Internet privacy protection and the corresponding scenarios are as follows:

Main concerns of privacy protection	Application Scenario	Risk Level
Biological monitoring information of operators	Various XR auxiliary operations	High
Analysis of operation record	Auxiliary Analysis of Operation Records	Medium
Biometric information	Identification and Verification	High
Operator identification information	Identification and Verification	Medium
Cloud data security	Industrial Internet Cloud Service	High

3.2.4. Mega Video and Cloud XR

[Application Scenario Overview]

Mega Video and Cloud XR (VR/AR) business application mainly relies on the large bandwidth of 5G network. Typical application includes 8K/4K live video, cloud XR games, video conferencing, high definition remote teaching, etc., all of which require bandwidth guarantee of 5G network. During the prevention and control of COVID-19, high definition video has presented its positive role in the medical field.

[Data Processing Analysis]

Mega Video and Cloud XR have high requirements on network bandwidth. Video rendering is often placed in the edge cloud computing, which reduces the pressure on the aggregation layer transmission and reduces latency. Mega video business has been applied in many fields, and the main participants are pan-entertainment platforms, mega video solution providers and cloud platforms providing basic resources. XR, as the terminal device of mobile cloud, presents the source signal with intuitive experience through large bandwidth transmission. Meanwhile, it can use the biometric information identified by wearable devices as the interaction signal between devices to drive the realization of application functions. Wearable devices connect people, affairs and objects with the Internet more and more closely. It records users' health index, life preference, behavior habits, movement track and other information, and personal privacy protection is facing increasing challenges.

Mega Video and Cloud XR mainly includes personal data types as below:

Data Categories	Data Types	Potential Data Controller / Processor
Biologic information	Facial recognition information, health information, fingerprint, voice print, iris, movement information, etc.	Mega video playing platform, APP, live broadcast platform, website, mega video solution provider

Equipment information	Terminal equipment code, etc.	Video terminal equipment provider, large video solution providers, application platform
Location information	Movement track, route, etc.	Mega video playing platform, APP, live broadcast platform, website, mega video solution provider
Internet browsing history	Operation log, favorite list, personal preference, etc.	Live broadcast platforms, websites, mega video solution provider
Financial information	Bank card accounts, payment records, etc.	Live broadcast platforms, e-commerce platform, banks, and finance-relevant service provider
Special information	Children data, etc.	Mega video playing platform, APP, live broadcast platform, website, mega video solution provider

[Main Concerns]

Main concerns of Mega Video and Cloud XR privacy protection and the corresponding scenarios are as follows:

Main concerns of privacy protection	Application Scenario	Risk Level
Facial recognition, voice print recognition, fingerprint recognition and other biometric information	Sound picture screen during live broadcast, personal identification function in security products	High
User health information	The information reflecting biological signs of natural persons in the wearable devices, which may also form functional interaction with other applications, such as payment, decoding, etc.	High
Children data	Internet education applications, online classroom	High

[Related Cases]

In November 2017, it was revealed that Strava, a wearable device, leaked users' privacy. Strava is an outdoor fitness tracking app that is popular in Europe and the US. Its main function is to put cyclists' performance results into the same ranking as those of famous athletes, so that they can compete with the world's best. Strava released a heat map of user activity around the world, with 1 billion activity tracks and 10 terabytes of input data. Internet users deduced the Australian military's exercise routes from Strava data, and further revealed hidden military bases around the world, with China included. Strava has a privacy setting feature that allows users to create a 1km radius of privacy area where their track disappears to hide where they live or work. Unfortunately, this feature is turned off by default, and very few users turn it on voluntarily. From the perspective of privacy by design (PbD), privacy protection function should be turned on by default to reduce unnecessary privacy risks.

3.2.5. Telemedicine

[Application Scenario Overview]

The large bandwidth and low latency of 5G network provide necessary mobile network support for smart medical treatment and promote the development of intelligent medical treatment. Main application scenarios include:

1) Remote consultation: by connecting the resources of medical institutions, remote high-definition video dialogue can be realized, disease information can be shared, patients can be detected remotely, and valuable treatment opportunities can be obtained for rapid diagnosis. The transmission of high-definition video requires 5G networks to provide the network foundation. Such services require full coverage of 5G networks in hospitals, with bandwidth of more than 40Mbps.
2) Remote ultrasound: primary-level hospitals generally lack excellent ultrasound doctors, while 5G network can realize high-definition and delay-free remote ultrasound examination, and also benefit remote areas where it is difficult to build special lines. Remote ultrasound requires full coverage of the hospital with 5G network

and a delay of less than 20ms.

3) Remote training: the level of medical treatment varies among regions in China, and the training cycle of doctors is long. Medical experts can conduct remote teaching through 4K/ 1080P high-definition teaching and various interfaces to connect with surgical field equipment. At the same time, there are many interactive teaching methods, and individuals can listen to lectures in various ways: computer, smart phone, intelligent AR or MR (Mixed Reality) glasses, etc. Remote training requires full coverage of hospital consultation rooms and bandwidth of more than 100Mbps.
4) Remote surgery: The surgeon can remotely control the surgical instrument and complete the surgery by sending back high-definition video content. Remote surgery requires full coverage of the operating room and a delay of less than 10ms.

[Data Processing Analysis]

Telemedicine involves a large number of patients' sensitive personal data, and there are many parties involved in data collection and processing. There are overlapping and ambiguous legal relationships and rights and obligations among these parties, which makes it more difficult to clarify the data protection obligations and responsibilities of each party. In addition, medical data generally need to be stored for a long time, data processing chain is long and there are many nodes, hence data asset management is difficult, and there are also many restrictions and uncertainties for users to exercise rights. Due to the public service nature of medical services, all parties are concerned about the security and legitimate use of medical data.

Telemedicine mainly includes personal data types as below:：

Data Categories	Data Types	Potential Data Controller / Processor
Basic identity information, basic personal information	Name, ID number, gender, ethnicity, family relationship, address, telephone number, social insurance card, residence permit, etc.	First-visit hospital, consultation hospital, social insurance institution, commercial insurance company, etc.
Personal physiological health information	Records related to personal medical treatment, e.g. illness, hospitalization records, the doctor's advice, inspection reports, surgery and anesthesia records, nursing records, medical records, medicine & food allergy information, maternity information, diagnosis and treatment records, family illness history, history of infection, etc., as well as personal health information, e.g. weight, height, lung capacity, etc.	First-visit hospital, consultation hospital, insurance institution, intelligent medical platform, etc.
Information collected by monitoring equipment or wearable equipment	Heartbeat, heart rate, sleep, exercise, blood pressure, blood oxygen, blood sugar, body temperature, etc.	Equipment supplier, device App developer, hospital, insurance institution, etc.
Medical consumption records	Bank accounts, passwords, payment records, etc.	Bank, payment service provider, hospital, social insurance institution, etc.

[Main Concerns]

Main concerns of Telemedicine privacy protection and the corresponding scenarios are as follows:

Main concerns of privacy protection	Application Scenario	Risk Level
A large number of patients' health and physiological data	Remote consultation, remote	High

and transaction records in hospitals are sensitive personal data that need special protection.	surgery, remote monitoring, etc.	
In the Telemedicine scenario, personal data is transferred among hospitals, social insurance institutions, insurance institutions, smart device hardware and software suppliers, etc. Involved parties are numerous.	Wearable devices, remote training, remote consultation of doctors	High
In addition to being used for medical purposes, personal data collected in Telemedicine scenarios may also be used for commercial insurance sales and grading, medical statistical analysis, remote training, and medical service advertising portrait, etc.	Wearable devices, , remote training, remote diagnosis and treatment	High

[Related Cases]

1) In October 2017, it was exposed that 47GB of medical data was leaked from Amazon database, and as estimated, at least 150,000 patients were affected. The leaked information includes patient blood test results, and personal information, such as patient's name, home address, doctor's information and illness case management records.
2) In March 2019, nearly 20 million payment records were leaked by the Medical Collection Agency, a US medical institution, including overdue payment records of laboratory customers and sensitive information such as social security numbers and bank account information.
3) In September 2019, the suspected breach of China's medical PACS server involved nearly 280,000 Chinese patient records, including personal data and medical details: name, date of birth, date of examination, scope of investigation, type of imaging procedure, attending physician, institute/clinic and number of images generated.

3.2.6. Intelligent Security

[Application Scenario Overview]

With the development of smart security, the security system has been gradually upgraded towards digitalization, networking, and intelligence. Along with the development of the Safe City and Xueliang projects throughout the country, the security industry has gradually spread from private fields such as public security and government to various civil fields, and penetrated into the lives of the masses. The main application scenarios of Intelligent Security include: The facial recognition technology is used to analyze High Definition camera (HD camera) images in public areas, so that suspects can be identified quickly and efficiently. During the security patrol of law enforcement personnel, the front-end camera or mobile phone is used for capturing and analyzing the personnel information to quickly identify the person. Major festivals in key areas, unmanned air protection patrol, and 360 degrees of monitoring places without blind spots, to ensure on-site security.

[Data Processing Analysis]

Based on the security solution for 5G networks, HD cameras are installed in public places to take real-time surveillance images, and upload HD images to the intelligent analysis server in real time. The server analyzes and processes images, and reports alarm information to the unified platform. Patrol personnel carry smart AR electronic glasses, take pictures in real time, transmit them to the smart analysis server through the 5G network to check the identities of suspected persons, and notify security personnel when the suspicious are found. In large concerts, gymnasiums, parks, and other densely populated places, drones are used to collect real-time images of the on-site for supplementary coverage monitoring, transfer the real-time images to the intelligent analysis server, and notify security personnel if any abnormality is found.

Intelligent Security mainly includes personal data types as below:

Data Categories	Data Types	Potential Data Controller / Processor
Basic ID	Name, ID No., family address, license plate number, etc.	Local public security organs, government agencies, organizations and enterprises that develop, deploy or use Intelligent Security technology systems
Biometric information	Facial recognition data, fingerprint, etc.	Local public security organs, government agencies, organizations and enterprises that develop, deploy or use Intelligent Security technology systems
Location big data	Location Information	Local public security organs, government agencies, organizations and enterprises that develop, deploy or use Intelligent Security technology systems
Other sensitive information	Children information, criminal records, etc.	Local public security organs, government agencies, organizations and enterprises that develop, deploy or use Intelligent Security technology systems

[Main Concerns]

Main concerns of Intelligent Security privacy protection and the corresponding scenarios are as follows:

Main concerns of privacy protection	Application Scenario	Risk Level
Legitimacy requirements of data processing	No monitoring device shall be installed in the space involving privacy in public places. The installation position of the camera part shall be clearly marked, so that the public can know the existence of the monitoring device.	High
Processing of biometric information, such as facial recognition and fingerprint recognition	Security inspections is carried out on natural persons entering the monitoring scope, focus on prevention controls should be conducted to check the identities of the suspicious.	High
Children personal data handling	During security monitoring, the system collects and handles children's and other adult's personal information.	High
Data storage security	The data collected through the security protection system contains a large amount of sensitive data, which is stored in local police stations or government agencies with different degrees of data protection.	High
Data sharing	Public security organs and government departments would share big data.	High

[Related Cases]

In May 2019, the world's first legal case of police used AFR Locate, a facial recognition technology. South Wales police processed public faces obtained from CCTV in real time, extracted facial recognition information, and compared it with those on the monitoring list. If the matching fails, the data is not stored. The data related to successful matching is saved for a maximum of 24 hours. CCTV records would be kept for 31 days in accordance with related standards. In February 2019, the MongoDB database of Deep Networking Technology Co., Ltd. did not

impose access restriction, resulting in data leakage of more than 2.5 million persons. The data types include facial recognition image, image shooting location, ID number, country, address, birthday, photo and location within the past 24 hours.

3.2.7. Intelligent Grid

[Application Scenario Overview]

The Intelligent Grid, together with 5G, MEC, and big data technologies, is mainly used in the following scenarios: Realizing synchronous phase measurement, differential protection, automatic power distribution, and advanced metering in the power distribution network, and achieving fault identification, location, isolation, and self-healing millisecond response. Drone, smart robot, video surveillance, and other service applications are launched to conduct real-time transmission of power operation inspection videos, and conduct Intelligent fault identification, analysis and prediction with the combination with AI. Power distribution terminals are ubiquitously connected to intelligent management to achieve the ubiquitous connection of the "last mile" of multi-faceted equipment. Through end-to-end network slicing services, 5G can meet the service communication requirements of smart grids, provide differentiated network services, and achieve secure isolation of resources.

[Data Processing Analysis]

In the application of Intelligent Grid, the service scenarios involving personal data mainly include such activities as smart meter-related metering and AR auxiliary maintenance/repair. Intelligent Grid usually collects meter data at high frequencies, including IP addresses of smart meters and real-time power consumption data, and on this basis, further mining and analysis of user requirements and habits may be performed. Real-time power consumption data has stronger privacy attributes.

Data Categories	Data Types	Potential Data Controller / Processor
User ID	User identity, account information, payment information, etc.	Electricity companies and cloud service providers
Smart terminal information	Terminal ID, IP address, power consumption data, real-time power consumption data, etc.	Electricity companies, equipment manufacturers, operators, and cloud service providers
Data profile	User requirements, user habits, etc.	Electricity companies, equipment manufacturers, operators, and cloud service providers
AR task information	Operator's identity, location, biological health information, etc.	Electricity companies, equipment manufacturers, operators, and cloud service providers

[Main Concerns]

Main concerns of Intelligent Grid privacy protection and the corresponding scenarios are as follows:

Main concerns of privacy protection	Application Scenario	Risk Level
User profile	Portraits of user requirements and habits	High
Processing of biometric information, such as facial recognition and fingerprint recognition	Auxiliary AR operations	High
Data security management	Storage and usage management of privacy	High

	information	

3.2.8. Intelligent Transportation

[Application Scenario Overview]

Intelligent Transportation uses smarter positioning devices, integrated analysis of big data, and more vivid visual means to further improve city management efficiency. The main application scenarios include:

1) **Smart travel:** to fulfill ticket purchase and query demands, detect the passenger traffic and conduct personnel distribution.
2) **Train operation:** to collect the position, status, and image monitoring information of a train, to control and dispatch the train intelligently, and to improve the efficiency of train operation.
3) **Facilities maintenance:** to analyze mass detection and alarm data, to reasonably schedule maintenance plans, to arrange maintenance personnel in a timely manner when an emergency fault occurs, and in special occasions, to conduct troubleshooting with remote experts guiding.
4) **Emergency disaster prevention**: in case of a security incident during a crowded rail transit, to dispatch emergency rescue team to respond immediately.

[Data Processing Analysis]

5G networks are deployed at Intelligent Transportation sites, tracks, and parking lots: Rail transit sites collect monitoring images in real time through 5G networks, analyze human traffic and passenger information, and implement intelligent travel distribution processing. This function is used to obtain train operation monitoring information, train status, and train control, and complete the facility maintenance procedure. The train operation data is transmitted to the data analysis server through the 5G network in real time to analyze and predict mass detection data and cooperate in equipment monitoring. The maintenance personnel complete troubleshooting in accordance with the 5G network and the connection guide mode recommended by remote experts. The monitoring images transmitted in real time through the 5G network use AI for facial recognition. If a suspected person is found, security personnel would be notified to handle the case immediately.

Intelligent Transportation mainly includes personal data types as below:

Data Categories	Data Types	Potential Data Controller / Processor
Basic Information	Name, ID number, telephone number, family address, etc.	Local public security organs, government agencies, and traffic operators
Biometric information	Facial recognition data, fingerprint, etc.	Local public security organs, government agencies, and traffic operators
Location big data	Location information	Local public security organs, government agencies, and traffic operators
Other sensitive information	Children information, criminal records, etc.	Local public security organs, government agencies, and traffic operators
Other Information	Handset signaling, travel paths, personal preferences, etc.	Local public security organs, government agencies, and traffic operators

[Main Concerns]

Main concerns of Intelligent Transportation privacy protection and the corresponding scenarios are as follows:

Main concerns of privacy protection	Application Scenario	Risk Level
Location Information	Locating passenger flow and passenger location, user smart travel, etc.	High

Processing of biometric information, such as facial recognition and fingerprint recognition	Preventive maintenance and key protection is conducted for natural persons, and identities of suspected persons are checked when entering the active range of rail transportation, etc.	High
Children personal data handling	During rail transportation monitoring, children's information and other adult's personal information are collected and processed in a unified manner, etc.	High
Data storage security	The Intelligent Transportation system collects a large amount of complicated data, including a large amount of sensitive data stored in transportation departments or local government agencies with different data protection security capabilities, etc.	High
Location data sharing	The transportation departments, public security organs, and government departments share big data across departments, etc.	High

3.2.9. Intelligent Airport

[Application Scenario Overview]

Smart airports include terminal buildings, VIP halls, aprons, and logistics centers. Service requirements in different places are diversified. The main service application scenarios are:

1) **Video entertainment services provided in VIP hall and terminal building:** Local VR/video hot content are provided with better user experience with high definition and low latency. VR game servers are deployed in edge cloud to provide game services with low latency and high image quality.
2) **Security application scenario of airports:** Law enforcement personnel carry AR smart glasses to take pictures in real time, so they can quickly identify suspected persons.
3) **Security robot Automatic patrol inspection:** Security robot runs according to the preset route, transmits videos to the analysis server in real time, and returns the analysis results to law enforcement personnel for quick response.
4) **Smart cleaning:** Manual cleaning of airports is time-consuming. In smart cleaning, operators use 5G networks to control robots to automatically clean airports, saving human resources and improving cleaning efficiency.
5) **Autonomous driving:** The driving lines of airport vehicles are relatively fixed. It is suitable to adopt the Vehicle to Everything (5G-V2X) scheme for automatic driving decision-making at different levels. The vehicles that are used in such scenarios as minibuses, ferries and commuters can fully share the 5G network coverage and intelligent infrastructure, thus reducing the operation cost and improving the operation efficiency of the airport.

[Data Processing Analysis]

Data processing participants of Intelligent Airport include airport operators, customs border control, security companies, airlines, banks, VIP hall operators, stores, passenger transport companies, express companies, and big data platform suppliers. The data subjects include passengers, airport personnel, and transport personnel.

Intelligent Airport mainly includes personal data types as below:

Data Categories	Data Types	Potential Data Controller / Processor
Basic passenger information	Name, ID number, flight number, seat number, and facial recognition data	Airport operators, customs border control, airlines, and big data platform suppliers, etc.
VIP customer service information	Name, ID number, bank card number, asset bank, asset compliance, flight mileage, habits of VIP halls, travel time rule, and catering hobbies	Airlines, banks, VIP hall operators, and big data platform suppliers, etc.
Security check information	Name, ID number, facial recognition data, and criminal records	Airport operators, customs border checks, security companies, and airline big data platform suppliers, etc.
Other Information	Shopping habits, membership card information, travel information, sender name, address, and phone number	Airport operators, airlines, stores, passenger transport companies, express companies, and big data platform suppliers, etc.

[Main Concerns]

Main concerns of Intelligent Airport privacy protection and the corresponding scenarios are as follows:

Main concerns of privacy protection	Application Scenario	Risk Level
Personal location information and personal track information	Security monitoring: Holographic and HD video monitoring has triggered privacy protection issues such as necessity, balance of interests, permission control, and data security.	High
Biometric information such as facial recognition, voiceprint, and fingerprint	Check-in/check-out management, port entry and exit, border inspections, and other security protection requirements shall be implemented for the staff, and the work status of the staff shall be monitored in real time and analyzed intelligently.	High
User profile	User profiles are formed through VIP service and shopping habits, so that commercial advertisements and customized services can be pushed to specific groups of users.	High

[Related Cases]

In October 2018, British privacy supervisory authority (Information Commissioner's Office, ICO) fined Heathrow Airport a sum of 120,000, starting with a USB flash disk containing sensitive airport security information that was found in the streets of London in October 2017. The basis of ICO punishment is the personal information of 1% in the data of USB falsh disk. A video clip exposes the detailed information of 10 members in a welcome team and the information of 12-50 security personnel. The information exposed in the video includes the name, birthday, registration number, nationality, passport number, validity period, position, and mobile phone number. After the incident occurred, Heathrow Airport hired third-party experts to monitor the secret network and the internet to find the evidence of the leaked data being sold on the Internet. Although no sign of data disclosure was found, ICO issued a ticket due to privacy management problems at the airport.

3.2.10. Intelligent Finance

[Application Scenario Overview]

The 5G network promotes the development of financial intelligence, and the front-end services are optimized to improve customer experience. The back-end system is centralized to improve efficiency and prevent risks. The main application scenarios include:

1) **Smart branches:** To improve customer experience, the system uses the self-serving robot to enable customers to complete services on their own. On the other hand, smart monitoring is used to analyze AI expressions, identify customer standards, accurately serve customer demands, and identify potential risks to ensure customer and bank security.
2) **Remote virtual banks:** Customers use VR devices to experience new virtual banks through 5G networks, thus saving customer time without physically entering banks.
3) **Mobile payment:** Based on the 5G+MEC network, mobile payment can meet the low-latency and high-bandwidth requirements of the cloud VR technology, provide richer decision data and more real scenarios for payment, and change the existing payment experience.
4) **Hewlett-Packard finance:** Hewlett-Packard finance converges and explores massive personal data and enterprise data to avoid risks caused by information asymmetry and promote the balance of financial services.
5) **Wealth management:, B**ased on the 5G network, big data analysis is conducted to provide precise portraits for each customer and provide the customer with extensive services.

[Data Processing Analysis]

The most direct change in 5G empowering the financial sector is the massive collection and analysis of data. While enjoying more efficient and convenient financial services, financial institutions and payment institutions can make portraits more accurate for individuals. Through personal habits and property status, they can precisely recommend related financial services and products, and people's property status is almost transparent.

Data Categories	Data Types	Potential Data Controller / Processor
Personal wealth data	Financial account data, transaction data, credit data, property data, and associated account information	Financial institutions, financial service software providers, and credit institutions
Biometric data	Fingerprint, voiceprint, and facial recognition data for identity verification	Financial institutions and identification service providers
Consumption data	Consumption records, transaction details, and user profile data	Consumption platform, payment institution, and financial institution

[Main Concerns]

Main concerns of Intelligent Finance privacy protection and the corresponding scenarios are as follows:

Main concerns of privacy protection	Application Scenario	Risk Level
Personal property information, financial account data and biometric data are sensitive personal data requires special protection.	Smart Investment and Smart Bank	High
Property data, credit data, and consumption data are associated, and precise financial services and products can be recommended to individuals.	Smart Investment and Smart Bank	High

3.3. Enlightenment of Privacy Protection in 5G Application Scenarios

5G is fully integrated with big data, cloud computing, AI, IoT, and other technologies to form various application scenarios. While developing value based on these scenarios, promoting economic and social development, and

serving people's lives efficiently, high attention needs to be paid to privacy protection and put into practice. Form the subjects' point of view, the privacy protection shall be built in a systematic manner, and the policies and resources shall be defined and clarified. A team shall be established, management systems and implementation guidelines shall be established, and awareness training and skill education shall be conducted. Necessary tools, systems, and technologies shall be provided to ensure the implementation. From the practical point of view, the basic principles of privacy protection shall be clarified, the compliance of privacy processing procedures shall be improved, high-risk scenarios shall be controlled, and the privacy concerns of new technology applications shall be focused on.

3.3.1. Basic Principles of Privacy Protection

In the collaboration with relevant parties in the 5G application scenario, they should focus on applicable laws and regulations, such as the China Cyber Security Law, Data Security Law, Personal Information Protection Law, Personal Information Security Regulations, Data Security Management Regulations, Personal Information Exit Security Evaluation Regulations, Children's Personal Information Protection Regulations, GDPR in Europe and CCPA in the US. Basic privacy protection principles include the following:

- **Lawfulness, fairness and transparency**: Personal data is processed in a legal, fair and transparent manner.
- **Purpose limitation**: The collection of personal data has specific, clear and proper purposes. The processing of personal data should not violate or exceed the initial purposes.
- **Data minimization**: The personal data, processed for the purpose of data processing, is appropriate, relevant and necessary.
- **Accuracy**: Personal data should be accurate. Reasonable measures should be taken to clear or correct inaccurate personal data in a timely manner.
- **Storage limitation**: The storage time of personal data shall not exceed the time required for the purpose of handling, and shall be disposed upon expiration.
- **Data integrity and confidentiality**: During the processing of personal data, reasonable measures should be taken to ensure security and avoid unauthorized processing of data and data breach.
- **Accountability**: Above requirements shall be complies with and corresponding compliance evidence shall be provided.

3.3.2. Requirements for the Data Processing Process

In the collaboration with relevant parties for 5G application scenarios, the management of the full lifecycle of personal data processing should be focused on. For example, to achieve transparency and earn trusts, the purpose, method, and scope of data processing should be informed. Multiple technical means including de-identification are used to protect the privacy and security of users. Data subject request response mechanism, data security emergency response mechanism, and audit system shall be established. The requirements for the data processing include:

- **Collection:** To meet the legality and minimization requirements, the data subject shall be able to choose, provide consent freely.
- **Storage:** To ensure data storage security, de-identification shall be conducted for data storage preferentially, and the storage retention should meet the storage limitation requirement. Data shall be disposed upon the data retention period.
- **Use:** The use of permissions shall meet the principles of responsibility necessity and least privilege. The data usage and scope shall meet the principle of purpose limitation and data minimization and shall not

be used for other than the initial purposes. For processing activities that may cause significant impact on data subjects, such as automatic decision-making, privacy impact assessment shall be conducted.

- **Deletion:** data storage management mechanism shall be established, and Data shall be disposed upon the data retention period.
- **External provision:** When private data is provided to external entities, such as entrusted processing, sharing, transfer, and public disclosure, privacy impact assessment must be performed in advance to ensure that the receiving parties have the corresponding privacy compliance capabilities. The receiving parties' privacy compliance responsibilities and obligations are stipulated through agreements or contracts, and their handling is evaluated and supervised.
- **Cross-border data transfer:** When applicable (for example, in the case of cross-border transfer of large-scale and highly sensitive private data), the request shall be submitted to supervisory authority for approval in advance. The Privacy Impact Assessment shall be conducted, and the responsibilities and obligations of the Receiving Party shall be specified through agreements or contracts, and the data processing shall be audited.
- **Data subject rights guarantee mechanism:** An effective mechanism shall be established to respond to the data subject right requests in a timely manner.
- **Privacy by design:** Privacy protection requirements shall be embedded in the design of products and service solutions at the beginning, and the privacy protection objectives are achieved in the best way through the comprehensive use of technologies, management, and physical measures, ensuring the security and compliance of the full lifecycle of privacy information.
- **Privacy security incident response: D**ata security incident handling process shall be established, emergency plans shall be formulated, personnel training shall be organize organized, and regular rehearsals shall be conducted.
- **Process review and regular audit: A r**eview and audit system shall be established to ensure the implementation of privacy compliance and improve the maturity of compliance capabilities.

3.3.3. High-Sensitive Data Processing for Privacy Protection

In the collaboration with relevant parties in 5G application scenarios, the application and privacy compliance of high-risk sensitive data should be focused on. Common high-risk sensitive data includes:

3.3.3.1. Accurate location information

[Overview] Accurate location information, mobility data, or movement information is the data element that describes the locations of devices and personnel in the aspect of movements in space over time. Accurate location information includes private information such as home and working addresses, and other sensitive information such as user habits, hobbies, health status, and social status. Improper use of location information poses a serious threat to user privacy.

[Legislative Enforcement] Accurate location information is legally sensitive data. In most jurisdictions, location data is special data that should be subject to higher protection and requires explicit consent and higher security standard.

- **China:** Article 28 of the Personal Information Protection Law clearly specifies sensitive information of movement, which can only be processed for a specific purpose, for sufficient necessity and under strict protection measures. At the same time, the position information "movement track" is written into the personal information of citizens protected by the criminal law. If the volume of illegal acquisition,

collection, or provision of movement track information provided to others reaches 50 records, the offense can be convicted and punishable: A maximum of one million fines could be imposed as required.

- **Europe:** In the European Union, the acquisition of location information is usually regulated by the telecom secrecy, and is strictly regulated by the ePrivacy Directive, which requires the consent of individuals (with few exceptions). Some member states have issued relevant requirements and guidelines on location information. In July 2019, the Commission Nationale de l'information et des Libertes (CNIL) specified in the user guide to Cookies and other tracing settings that the operator should not read or write any data in the user terminal until permission is obtained.
- **The United States: T**he U.S. Federal Trade Commission has long required affirmative approval of the location information requirements.The protection of location information in various states has also been put on the agenda. New York City is enacting a bill to prevent mobile phones and app companies from sharing their collected user location information without consumer consent.

[Privacy Protection Compliance] When using location information, in addition to the basic privacy protection principles that must be followed, data shall also be de-identified or anonymized as much as possible, and the processing data shall be controlled within the minimum necessary range. In addition, when providing external location information, the information sharing shall be clearly described through the privacy policy to obtain the explicit consent. When precise location information is used for public interests, for example, citizen location information is collected after relevant authorization is obtained in early epidemic prevention and control, the purpose and scope of information usage, storage time, and data disposal shall be considered. If the initial purpose is to track an epidemic, the location information shall not be retained for other purposes after the epidemic prevention and control are completed.

[Related Cases] Associated Press's investigation into Google shows that Google is still collecting user location information when users choose to disable the location service or location history records, which is suspected of misusing the user's personal data. For example, the Google Map application notifies a user that the user is allowed to use geographical location information for navigation services. If the user agrees, the Google map displays the historical record (daily geographical location of the user) on the “time axis”. Google provides the option of disabling the location record for users in the dashboard. After closing the location record, Google will no longer store the user's geographical location information. However, according to an investigation by the Associated Press, even if location records are disabled, some Google apps automatically store geographical location data with timestamps without user permission. In addition, even if all location services are disabled, Google can track the locations of Android users by collecting the addresses of nearby mobile phone signal towers.

3.3.3.2. Accurate user profiling

[Overview] In various 5G application scenarios, user accurate portraits and personalized recommendations have become more and more common. More and more enterprises are collecting personal browsing records, purchase records, and transaction methods, analyzing user behaviors, and carrying out accurate portraits and marketing of users based on the information. An user profiling is a complete user profile that is abstracted by collecting and analyzing consumer social attributes, habits and behaviors. The focus of a user profile is to label the user. A label is a highly refined personal identity defined manually, such as age, sex, area, and user preference. Finally, all the labels of the user are summarized to provide a three-dimensional profile of the user. User profile labeling and personalized recommendation pose challenges to user privacy protection.

[Legislative Enforcement] Different countries and regions have adopted different legal regulations for user

profiling.

- **China:** Article 24 of the Personal Information Protection Law specifies the requirements for the transparency, impartiality, and prohibition of unreasonable differential treatment for the information push derived from automatic decision-making. For the information push and commercial marketing that are made through automatic decision-making, the information shall also be provided with the options that are not based on personal characteristics, or convenient rejection modes for individuals. Article 18 of the E-Commerce Law stipulates that If a business operator provides search results of goods or services to consumers in accordance with their interests, hobbies, and consumption habits, it shall provide the consumers with options that are not based on their personal characteristics, and respect and protect the legal rights and interests of consumers. The above regulations are applicable to user profiling. It is clarified that the decision-making behaviors on the basis of user profiling shall meet the requirements of legality, transparency, and fairness.
- **Europe:** The EU GDPR specifically regulates the user profile, especially imposes multiple obligations on the user profile processing of data controllers, and grants multiple data rights to the data subject to reduce and eliminate privacy protection risks and impacts.
- **The United States:** At the federal level, there is no legal regulation on the use of consumer behavior by websites to make user profiling and personalized recommendations. However, the Federal Trade Commission of the United States published a report in 1998, which comprehensively reviewed the disclosure of user privacy on business websites and developed the Rule of Fair Information Practice (FIP). According to the FIP principle, when collecting personal information, the website needs to provide consumers with clear and explicit information of their information processing, including what information is collected, how information is collected (such as cookies), how the data is used, how choices are provided with consumers , accessibility and security, whether data collected is disclosed to other entities, and whether other entities are collecting information through the website. Guided by the principles of fair information practice, the Federal Trade Commission (FTA) adopts a transparent-based regulatory principle, namely, when a website violates privacy policies to collect personal information or when the website is opaque about personal information collection, the FTA may require the website to comply with the requirements for transparency in information collection.

[Privacy Protection Compliance] In the process of data collection, analysis, judgment, or prediction for user profiling purposes, in addition to the basic privacy protection principles, special attention shall be paid to the following aspects:

- **The consent notification requirement:** User should be granted the right to freely choose and make independent decision. For example, when the website collects user behavior data by using technologies such as Flash Cookie, Ever Cookie and Fingerprint, a clearer notice shall be given to the user. The data can be collected only when the user has explicitly agreed to join in it.
- **Risk regulation principle:** Avoid using some sensitive data that may bother users. Even if an individual has explicitly provided consent for his/her behavior information collection, such sensitive data shall be restricted from accurate user profiling.

[Related Cases] A company launched the annual bill review function at the beginning of 2018. It has been found that using small fonts, proximity to the background, and default options at the bottom left of the front page of the annual bill, a considerable number of users "approved" without their knowledge. The signing of the service agreement, which is easily ignored by users, means that all the information of users would be analyzed and user profiling could be shared with other business partners / entities. This company apologizes to the public, adjusted the page, and canceled the default check box. In this case, the company violated users' rights to provide consent and to choose and violated the requirements of the Consumer Rights Protection Law, the Personal Information Security Regulations, and other regulatory standards by using small fonts and unclear font color, default selection

for users' consent and inducing users to ignore notification.

3.3.3.3. Biometric data

[Overview] Biometric data, also known as biometric identifiable features, refers to the information obtained by performing certain technical processing on the physical body, physiology or behavior of a natural person to identify him / her. Common physical body and physical information includes fingerprint information, palmprint information, facial recognition information, voiceprint information, iris information, gene information, and blood vessel distribution information. Behavior characteristics include handwritten signatures, keyboard input, and specific walking or speaking modes. Biometric data is unique. Once it is leaked, illegally provided, or misused, it will greatly damage the personal and property safety of the data subject.

Biometric data is widely used in social, consumer, transportation, and financial fields due to its convenience and speed. The specific application scenarios include electronic payment, access control, attendance management, and cell phone unlocking. Many 5G application scenarios may involve the processing of biometric data, such as Intelligent Security, wearable devices, Telemedicine, and Intelligent Transportation. The purpose and mode of data utilization should be combined to judge whether it constitutes the processing of biometric data. The following factors should be considered: (1) The nature of the data: Data related to the physical, physiology or behavioral characteristics of a natural person. (2) Method and processing: The data originates from specific technical processing. (3) Purpose of processing: The data must be used for the specific purpose of identifying a natural person.

[Legislative Enforcement] There is a large difference in the legal regulation of biometric data in different countries. Laws and regulations in most countries and regions consider biometric data as sensitive data, and strictly restrict the use of biometric data.

- **China:** The Personal Information Protection Law and GB/T -2020 Personal Information Security Specifications define biometric data as sensitive personal information. To collect and use such information, it is required to obtain separate or explicit consent. GB/T 40660 Basic Requirements for Information Security Technology Biometric Information Protection lays down detailed regulations on the protection and management of biometric data. The Personal Information Security Engineering Guide for Information Security Technology (Draft) requires that irreversible protection shall be used when biometric data is used for identification. GB/T 39335 -2020 Personal Information Security Impact Assessment Guide requires impact assessment on biometric applications, and requires the compliance for the full lifecycle of collection, use, storage and destruction of biometric data.
- **Europe:** Clause 9 of GDPR strictly restricts the processing of special types of personal data, including biometric data, and the processing of biometric data shall be generally prohibited. Article 9 stipulates that member states can maintain or introduce further restrictions for the processing of genetic data, biometric data or data concerning health.
- **The United States:** Although there is no specific federal law regulating the collection and use of biometric data, section 5 of the Federal Trade Commission Act gives the Federal Trade Commission a wide range of enforcement powers to protect consumers against unfair and deceptive trade practices. Law enforcement is available to business organizations engaged in unfair or fraudulent trade practices involving biometric data. At present, seven states or cities have formulated laws related to biometric data, including Illinois, Texas, Washington, Summerville, Oregon and New Hampshire, and San Francisco, California. In 2008, Illinois passed the Bioinformation Privacy Act. In 2009, Texas passed the Law of Collection and Use of Biological Recognition Data. Other states are considering similar laws. The United States is gradually becoming conservative in the application of facial recognition technologies, such as San Francisco and Summerville.

[Privacy Protection Compliance] Biometric data is widely used in a wide range of application scenarios. In the absence of legal regulations on biometric data protection in China, the self-specification, self-discipline and self-improvement of enterprises collecting and processing biometric data can be achieved through the supervision of internal code of conduct, industry standards and industry associations.

In addition to the basic privacy protection principles that must be followed during the processing of biometric data, the following points shall be considered:

- **Minimization:** The use of biometric data such as facial recognition should be cautious. Such data can be used only when other methods cannot achieve business purposes. Otherwise, there will be high compliance risks. The excessive use of biometric data for social or commercial purposes should be strictly restricted.
- **Explicit consent:** Explicit consent of the data subject is obtained through clear, easy-to-understand and easy-to-access privacy statement.
- **Privacy impact assessment:** Privacy impact assessment shall be performed in advance, and handling measures for potential risks shall be formulated.
- **Privacy protection design:** For products or services involving biometric data processing, the privacy protection solution should be considered from the perspective of design sources to enhance transparency and minimize risks of violation.

[Related Cases] On August 20, 2019, a Swedish high school student was deemed to have violated the European General Data Protection Regulation by using facial recognition technology to record his/her attendance in class. A college or university in Nanjing is installed with a facial recognition system for access control, attendance management, and records monitoring. Students could be sensed when they were in a daze and play mobile phones. Public opinion is aroused due to the suspected infringement of students' privacy. In September 2019, a domestic network store was found to sell 170000 pieces of face data.

3.3.3.4. Children Data Processing

[Overview] According to the 2019 National Research Report on the Internet Usage of Minors, China's underage Internet users have reached 175 million. Due to such a huge number of Internet users and the insufficient risk awareness and privacy protection awareness of children, criminals tend to use the Internet to infringe on the legitimate rights and interests of children and endanger their physical and mental health.

[Legislative Enforcement] Regulations are in place in many countries around the world to protect children's network rights and interests. In many 5G application scenarios, processing of children data may be involved, such as Intelligent Campus and wearable devices. Children privacy protection is an important issue that cannot be ignored.

- **China:** The Regulations on Personal Information Network Protection for Children has taken effect since October 1, 2019. Based on the Cyber Security Law and other general rules, China has stipulated stricter information protection obligations for children, and granted children and their guardians more comprehensive and powerful rights. In the Personal Information Protection Act that comes into effect on November 1, 2021, the personal information of minors under the age of 14 is regarded as sensitive personal information, and such requirements as separate consent for enhanced protection are raised.
- **Europe:** The European GDPR raised higher requirements for the protection of children's personal information. Article 8 of GDPR stipulates that before collecting or handling personal data for children under 16 years of age, the consent or authorization of their parents is required. The member states may set a lower age limit, but not lower than 13 years of age. Article 38 of GDPR preamble states that when children personal data is

used for marketing and data processing purposes such as digital profiling, special protection should be provided. Article 71 of GDPR specifically states that automatic decision-making based on digital profiling should not involve children.

- **The United States:** As the Federal Trade Commission frequently conducts investigations and accusations under the Children's Online Privacy Protection Act (COPPA), the settlement amount is also increasing, indicating that the U.S. places more emphasis on and children personal data protection.

[Privacy Protection Compliance] The particularity of children determines that enhanced protection should be provided for personal data of children. The legislation and practice mentioned above can provide compliance guidance for enterprises or organizations to deal with children personal data. For an enterprise or organization processing personal data for children, in addition to the basic principles of privacy protection that must be followed, the following points shall be considered:

- **Consent notification: T**he products or services of children shall be designed in accordance with the high-standard notification consent mechanism, including the formulation of special child data processing rules, full notification and acquisition of the independent consent of children's parents or guardians, identification of guardianship relationships, and validity of guardianship authorization. An enterprise or organization shall start with the characteristics of its own business mode, and design an effective identification and authentication mechanism to ensure that data processing activities have legal basis.
- **Data security:** Before collecting children's personal data, data protection impact assessment should be performed and effective measures to reduce risks and fully guarantee data security shall be taken.
- **Industry standards:** In accordance with the legislation and supervision arrangement of "Internet + education" in recent two years, the latest supervision requirements for education products, such as remote education Apps, shall be met. The network security and personal information protection systems shall be improved, and the corresponding technical measures shall be optimized to meet the supervision requirements of the education industry.
- **Child user classification management:** Child mode can be set for products and services oriented to all-age users, and the corresponding children's personal information can be stored independently to reduce the compliance risks of children's personal information protection.

[Related Cases] In February 2019, a settlement was reached with Tik Tok (Wobble International Version) for the violation of the COPPA bill, and Tik Tok was fined US $5.7 million. The charges against the company include: failure to show online child information collected, how the information is used, how the notification is disclosed, failure to notify parents directly, and failure to obtain parental consent before collecting the child's personal information. On September 4, 2019, the company imposed a fine of $170 million to Google for YouTube violation of the COPPA bill, which was the biggest bill that was issued by the company under COPPA. The authority for YouTube enforcement includes the failure to provide clear, understandable, and complete privacy policies for collecting children's information, and to obtain verifiable parental consent before collecting, using, or sharing personal information on children.

3.3.4. Privacy Concerns Of New Technology Applications

In collaboration with relevant parties in 5G application scenarios, the application of new technologies involves a series of privacy protection concerns. For details, below compliance recommendations shall be referred.

New Technologies	Major Privacy Concerns	Privacy Compliance Suggestions

IoT	● Multi-channel collection of high-dimensional data data ● Difficult consent notification without acknowledgement of data collection . ● Sensitive personal data acquisition, such as accurate location information, facial recognition information, child personal data etc.; ● Potential security risks easily to cause data leakage.	● Comply with the basic principles of privacy protection. ● Refer to the industry best practice and the notification and approval mechanism for high-standard design. ● Adopt the design and technology that enhances privacy protection capability, such as synchronous encryption, secure multi-party computing, K- anonymity and differential privacy. ● Enhance security management of the IoT, and improve the device and data security protection capabilities ● Strengthen the data protection impact assessment and privacy compliance audit. ● Improve the data breach response mechanism and data subject rights response channels.
Cloud Computing	● Dross-border data processing risk; ● Third-party data processing risks; ● Compliance risks with data opening and sharing; ● Data breach risk.	● Comply with the basic principles of privacy protection. ● Apply privacy protection technologies are to enhance data management and control, such as synchronous encryption, secure multi-party computing, federation learning, K-anonymity, differential privacy, ciphertext retrieval, blockchain and ABAC/PBAC access control. ● Clarify the rights and responsibilities of cloud service providers through contracts. ● Strengthen the data protection impact assessment and privacy compliance audit. ● Improve the data breach response mechanism and data subject rights response channels.
Big data	● Excessive data sources to cause compliance problems; ● Data de-identification; ● BIg data analysis and profiling; ● Automatic identification, inference, and decision making; ● Serious consequences of data breaches..	● Comply with the basic principles of privacy protection. ● Apply privacy protection technologies to protect original data, such as synchronous encryption, secure multi-party computing, federation learning, K- anonymization, differential privacy, ciphertext retrieval, blockchain and ABAC/PBAC access control. ● Strengthen the Data Protection Impact Assessment and privacy compliance audit. ● Improve the data breach response mechanism and data subject rights response channels.
AI	● Algorithm transparency and fairness; ● Strong data integration, analysis, and profiling capabilities; ● Training on data compliance issues; ● More hidden Information acquisition methods; More series consequences of privacy infringing.	● Comply with the basic principles of privacy protection and AI ethics, and avoid algorithm discrimination and solidification bias. ● Improve the description of algorithm processing rules. ● Apply privacy protection technologies to enhance data protection, such as synchronous encryption, secure multi-party computing, federation learning, K- anonymity, differential privacy, ciphertext retrieval, blockchain and federation learning. ● Strengthen the Data Protection Impact Assessment and privacy compliance audit. ● Improve the data breach response mechanism and data subject rights response channels.

Conclusion

Digital economy is accelerating the convergence and development of information technologies such as the Internet, cloud computing, artificial intelligence, blockchain, and the Internet of Things through information tools such as network infrastructure and intelligent devices. The human being's ability to process the quantity, quality, and speed of big data is increasing. It promotes the transformation of the social economy from industrial economy to digital and intelligent economy, which greatly reduces the social transaction costs, increases the value added of products, enterprises, and industries, and promotes the rapid development of social productivity. In addition, it also provides the possibility for developing countries to achieve superb development.

In the future, with the further empowerment of 5G communication technologies in all fields of social production and life, industry integration and application innovation will be accelerated, and become the acceleration engine of digitalization and intelligence of social economy. In the process of transforming into a digital economy, data becomes a core production factor parallel to land, labor, capital, and technologies, and plays an increasingly important role in economic development. The compliance application of data, especially personal data, has become a wide public concern.

Therefore, countries around the world are exploring how to balance the privacy protection of massive data with open sharing and maximize the potential value of data. The European Union GDPR, the United States' CCPA and China's personal data Law of Protection and the Data Security Law are all providing respective solutions for the compliance application of the personal data.

5G will undoubtedly open a new beginning for us. With the continuous improvement of privacy-related laws and regulations, standards and regulations, technical solutions, and industry practice, and the awakening and upgrade of citizens' awareness of privacy protection, and the growing concern about privacy protection, all walks of life have invested in privacy compliance. We believe that the challenges and difficulties facing will be properly solved.

A social ecosystem that advocates technology and respect for privacy represents the future. This requires the joint efforts of the whole society, including all parties related to the 5G industry chain, and the active exploration of privacy protection practices to jointly build an open, transparent, secure, and credible 5G application ecosystem. We believe that as 5G, the Internet of Things, and data centers are included in the national information infrastructure, the launch of the new infrastructure will accelerate data compliance construction and promote the arrival of the Internet of Things era.

5G APPLICATION SCENARIOS AND PRIVACY PROTECTION RESEARCH REPORT

Main Editors: Gao Ruixin, Song Weiqiang, Yang Yuxin, Ding Pei, Wang Zhiyu, Fang Yuan, Wei Andi, Pang Qiuming, Huang Hao, Chen Piaopiao, Mao Anna, Peng Huanhua, Yu Di

Co-editors: Qu Shenwei, Chen Zhengwei, Wang Jingfei, Wang Hongxin, Chen Chengbiao, Gu Bu