


Thematic Snapshot: Privacy Policies

In the ASPI ICPC policy brief [Mapping China's Technology Giants: Supply Chains and the Global Data Ecosystem](#) we note that it is standard practice for global companies to acknowledge in their privacy policies that user data may be transferred and governed by laws outside of their own jurisdiction. PRC-based technology companies themselves have acknowledged their exposure to legal risks emanating from the current data security system being developed in the PRC. Recent state security laws, like the 2017 Intelligence Law, have not changed the long-standing *de facto* practice of state power in the PRC, but have further codified the expectation that in the PRC everyone is responsible for state security.



For any company doing business in the PRC, this creates a set of political and legal risks. According to most privacy policies for websites and products of the 27 companies in our [Mapping China's Technology Giants project](#), users who live outside of the PRC may have their data transferred, processed, and stored, in a country which is not where they reside or have ordered services from, including the PRC where all of the companies have business. When the data is transferred it will be governed by law in that country's jurisdiction, not only the place where the data originated. For PRC-based companies with global operations, there are particular risks related to the ways the state could access and use data obtained from overseas users who may be unaware of the global data collection norms developing in the PRC.

COMPANY	PRIVACY POLICY PURPOSE	JURISDICTION POLICY	PERSONAL DATA DISCLOSURE
	<p>The privacy policy on Alibaba's international website applies to the 'collection, use and disclosure of information in connection with the products and services offered by Alibaba.com.'</p>	<p>Alibaba can transfer personal information 'to countries/regions outside of the European Economic Area (EEA), including to jurisdictions where the data protection level 'is different from that of [a customer's] home country, such as the United States and China.'</p>	<p>Alibaba 'may disclose (or provide) personal information to ... third-party business partners, service providers and/or affiliates'...'law enforcement agencies, governments and regulatory and other agencies, if [Alibaba] believe that it is necessary to comply with applicable laws.'</p>
	<p>The privacy policy on Alibaba subsidiary Alibaba Cloud's International Website states that it applies to 'how we collect, use, transfer, retain, secure and disclose your personal data and/or personal data about your customers or end users that you provide to us pursuant to your use of the Alibaba Cloud Platform and/or our Cloud</p>	<p>It says that Alibaba Cloud can transfer personal information 'to countries/regions outside of the European Economic Area (EEA), including to jurisdictions where the data protection level 'is different from that of [a customer's] home country, such as the United States and China.' The policy adds that as it relates to personal data received or</p>	<p>'In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.' Among the reasons the company lists for collecting, using and disclosing personal data are 'to comply with applicable law, legal process</p>

Mapping China's
TECH GIANTS

COMPANY	PRIVACY POLICY PURPOSE	JURISDICTION POLICY	PERSONAL DATA DISCLOSURE
	<p>Services, as well as other terms relating to data location.'</p>	<p>transferred pursuant to the EU-U.S. and Swiss-U.S. Privacy Shield frameworks, Alibaba Cloud US LLC and Alibaba.com LLC are subject to the regulatory enforcement powers of the U.S. Federal Trade Commission.</p>	<p>or lawful government request, or in respect of any claims or potential claims brought against us or our parent companies, shareholders, subsidiaries and affiliates; performing risk control, legal compliance and sanctions screening; and performing screening and checks for unlawful, fraudulent, deceptive or malicious activities.'</p>
	<p>Ant Group's privacy policy last updated in 2018 and published on Alipay.com covers its services such as Huabei, Ant Jiebei, Ant Fortune platform services, Ant Insurance platform services, Ant Forest, Ant Farm, and Easy Rent. Relevant service providers will collect, store, use and disclose the user's information in order to comply with the requirements of PRC laws and regulations as well as regulatory requirements.</p>	<p>It states that personal data collected and generated by Ant Group within the PRC will be stored in the PRC. In the case where relevant service providers are required to transmit personal data collected within the PRC to any overseas institutions, relevant service providers will follow the provisions of applicable laws and regulations and regulatory requirements and will require such overseas institutions to keep personal data confidential.</p>	<p>The policy says Ant Group may 'share, transfer, or disclose your personal data without seeking your consent' 'in order to comply with relevant laws, regulations and national standards" under circumstances including 'directly related to national security and defense.'</p>
	<p>In the privacy policy posted to Baidu's investor relations website, when a party uses Baidu servers, the company will 'automatically record certain information, including URL, IP address, type of browser, language used, and the date and time of visit, etc.'</p>	<p>It says Baidu can transfer personal data to 'locations outside of the territory where [customers] are accessing Baidu's services or disclosed to our related corporations, licensees, business partners and/or service providers for the purposes described above.'</p>	<p>According to the policy Baidu will disclose personal information 'as per the requirements of the relevant laws and regulations" and "as per the requirements of the competent government authority.'</p>
	<p>The privacy policy posted to Baidu USA's website covers</p>	<p>It disclosed that the data it collected 'may be stored and</p>	<p>It says Baidu can transfer 'information to China or the</p>


Mapping China's
TECH GIANTS

COMPANY	PRIVACY POLICY PURPOSE	JURISDICTION POLICY	PERSONAL DATA DISCLOSURE
	<p>its applications and online services such as TalkType, FaceYou, SwiftScribe, and Voice Recognition.</p>	<p>processed in China, the United States and any other country in which Baidu or its subsidiaries, affiliates or service providers maintain facilities.' For people located in the European Union or other regions with laws governing data collection and use that may differ from Chinese or U.S. law, Baidu may transfer information, including personal information, to a country and jurisdiction that does not have the same data protection laws as the jurisdiction where the person accessed the website from.</p>	<p>U.S. or any other country in which Company or its parent, subsidiaries, affiliates or service providers maintain facilities and the use and disclosure of information about [the person] as described in this Privacy Policy.' It says personal data may be disclosed to 'China or the U.S. or any other country in which Company or its parent, subsidiaries, affiliates or service providers maintain facilities.'</p>
 <p>BeiDou</p>	<p>In its privacy policy (in Chinese), BeiDou Map, one of BeiDou's services, states that users' information will be collected without consent in several instances, such as in cases involving national security, national defence security, public safety, public health and major public interest cases, and in other circumstances stipulated by laws and regulations. It seems to be only applicable in the PRC.</p>	<p>It states that the data it 'collects and generates within the territory of the People's Republic of China will be stored in the territory of the People's Republic of China.' 'Personal information may be transferred to the overseas jurisdiction of the country/region where you use the product or service.'</p>	<p>The policy says BeiDou will disclose person data under circumstances including 'in the case of laws, legal procedures, litigation or mandatory requirements of government authorities.'</p>
	<p>BGI has published a privacy policy covering their 'websites, mobile applications, and/or our genetic testing and sequencing services.'</p>	<p>BGI may transfer personal information 'outside of the country where [customers] live or have ordered [BGI] services.' This includes 'subsidiaries, affiliated companies and service providers located in other jurisdictions, and may</p>	<p>According to the policy BGI 'will never share or disclose personal information' without prior consent unless the information is directly relevant to national security or national defence security; it is relevant to public security, public health or significant public interest; or</p>


Mapping China's
TECH GIANTS

COMPANY	PRIVACY POLICY PURPOSE	JURISDICTION POLICY	PERSONAL DATA DISCLOSURE
		become subject to the laws of such jurisdictions.'	it is directly relevant to investigation, prosecution, trial and execution of judgment of crimes.'
	<p>According to the privacy policy for the ByteDance security centre, applied to users of the ByteDance security centre website, the company may collect, use and store personal information.</p>	<p>ByteDance stores information collected within the PRC in accordance with the provisions of laws and regulations.</p>	<p>The privacy policy states that ByteDance won't share data without prior consent except in the instances that ByteDance merges with another company; the data relates to national security, national defence, public security or public health; or ByteDance is required to provide the data to meet the requirements of relevant laws, regulations, procedures and judicial proceedings.</p>
	<p>CETC's overseas activities are research partnerships, R&D labs, and MoU agreements, rather than the export of digital technologies. The privacy policy we found is unlikely to be highly relevant to these activities.</p> <p>The privacy policy on CETC's China-based website applies to users accessing its website. The website automatically collects user IP and information browsed on the website.</p>	<p>The privacy policy does not address issues related to jurisdiction.</p>	<p>The policy states that CETC would not share any individual's information with any third-party organisations unless it were asked to provide information 'according to the laws, regulations, policies and other normative legal documents of the People's Republic of China' or 'to maintain the privacy and safety of users or the public under an emergency'.</p>
	<p>China Mobile's privacy policy is published through its Hong Kong-listed entity.</p>	<p>The company states that it may transfer, disclose, grant access to or share personal data with 'government and regulatory authorities and law enforcement agencies and other organisations, as required or authorised by law' in accordance with the</p>	<p>The policy says China Mobile may transfer personal data to within or outside Hong Kong, including to 'government and regulatory authorities and law enforcement agencies and other organizations, as required or authorized by law.' China Mobile may</p>



Mapping China's
TECH GIANTS

COMPANY	PRIVACY POLICY PURPOSE	JURISDICTION POLICY	PERSONAL DATA DISCLOSURE
		<p>Personal Data (Privacy) Ordinance (Cap. 486) of the Laws of Hong Kong Special Administrative Region.</p>	<p>disclose or share personal data with parties within or outside Hong Kong, including 'government and regulatory authorities and law enforcement agencies and other organizations, as required or authorized by law.'</p>
	<p>Based in Hong Kong, China Telecom has a set of privacy policies subject to Hong Kong law. According to this privacy policy which applies to use of China Telecom Global Ltd. website and services, the company will hold users' data on the companies' 'servers in Hong Kong China.</p>	<p>However, we may transfer it to our overseas offices elsewhere in the world.' The policy says the company will keep 'Personal Information we hold confidential but may provide it to the following for the above mentioned purposes and as set out below: our affiliates, subsidiaries and/or representative offices in Hong Kong China, China mainland, Australia, Indonesia, India, Japan, South Korea, Malaysia, Thailand, Vietnam, Singapore, Kazakhstan, the United States of America and Europe, which include, but are not limited to, China Telecom Corporation, China Telecom (Europe) Limited and China Telecom (Americas) Corporation.</p>	<p>This can also include persons to whom we are required to make disclosure under applicable laws in or outside Hong Kong.</p>
	<p>China Telecom (Americas)'s Privacy Policy pertains to the 'collection, processing, use, storage and disposal of information that we collect from and about any of our customers that may be 'personally identifiable.'</p>	<p>It says the company 'will share your personally identifiable information only with our affiliated group companies and to our selected business partners who act on our behalf in providing the services'. Customers consent to 'the transfer, storage and processing of such</p>	<p>The policy says that customers agree to allow China Telecom to 'disclose any information to law enforcement or other parties that we, in our sole discretion, believe is required or appropriate to comply with the law'.</p>

Mapping China's
TECH GIANTS




COMPANY	PRIVACY POLICY PURPOSE	JURISDICTION POLICY	PERSONAL DATA DISCLOSURE
		<p>information between our offices in the United States and our affiliates abroad as may be necessary in connection with our provision of international services.'</p> <p>The policy adds that China Telecom 'cannot control how third parties use information.' The policy states that for countries subject to the GDPR, information provided to the company 'may be transferred to and stored in countries outside of the European Economic Area (EEA). That includes being processed by employees operating outside the EEA who work for China Telecom or one of its suppliers.</p>	
	<p>The privacy policy covering China Unicom (Europe) Operations Ltd, posted to the China Unicom Global website, covers how the company deals with users' personal information when they are using its products, services or websites. The collection policy includes content data such as SMS, email, speech and so on collected for several purposes, including 'compliance with legal and regulatory obligations', and it may be disclosed to any law enforcement or other government agency. The information, according to the policy, may be transferred to and processed outside the user's country of residence. China Unicom (Europe) may disclose personal information</p>	<p>The information, according to the policy, may be transferred to and processed outside the user's country of residence.</p>	<p>China Unicom (Europe) may disclose personal information to 'any competent law enforcement body, regulatory, government agency, court or other third party where we believe disclosure is necessary (i) as a matter of applicable law or regulation.'</p>

Mapping China's
TECH GIANTS

COMPANY	PRIVACY POLICY PURPOSE	JURISDICTION POLICY	PERSONAL DATA DISCLOSURE
	<p>to 'any competent law enforcement body, regulatory, government agency, court or other third party where we believe disclosure is necessary (i) as a matter of applicable law or regulation.'</p>		
	<p>A Terms of Use statement posted to CloudWalk's website, which applies to 'all services provided by Cloudwalk,' states that to provide users' with particular services, it may need to collect specific information. This information includes, 'Data about the person to contact: Name, email address, phone number, company name, company type, nationality, position etc.; Login data: User name, password etc.; Transaction data: Accessing data and data necessary for operation etc; [and] Registration information: Relevant information provided by you at the time of registration.'</p>	<p>The privacy policy does not address issues related to jurisdiction.</p>	<p>The statement says that CloudWalk's 'website will not share your information with third parties without your prior consent. We may access, transfer, disclose and save your information under the following circumstances: (1) Comply with laws and regulations or relevant legal procedures, including law enforcement agencies or other government agencies; (2) In accordance with relevant terms of use of this website; (3) Operate and maintain the security of the website; (4) Protect the rights and interests of users of this website.'</p>
	<p>Dahua's privacy policy applied to those who visited https://www.dahuasecurity.com/, including any subdomains and any content, functionality and services offered on, by or through it or them, or any other websites, e-mails, applications.</p>	<p>Dahua's privacy policy states that user 'information might be transferred outside the region and country you use our Site and Services, including to regions/countries outside the European Economic Area ("EEA") which might have different legal rules and might not offer an adequate level of protection as determined by the European Commission.'</p>	<p>The policy adds that Dahua may disclose personal data 'with certain trusted third parties that perform business functions' or "to comply with any court order, law or legal process, including to respond to any government or regulatory request or for investigations.'</p>

COMPANY	PRIVACY POLICY PURPOSE	JURISDICTION POLICY	PERSONAL DATA DISCLOSURE
	<p>DJI's privacy policy, which was updated on 1 January 2020, applies to DJI Products and Services.</p>	<p>It states that the information DJI collects may be used 'to detect, prevent, and respond to fraud, abuse, security risks, and technical issues that could harm our users, us, or the public'. It says the information collected by DJI 'may be transferred to and accessed by DJI entities and business partners globally.' If user is located in the European Economic Area (EEA), then DJI GmbH in Germany is the data controller, and DJI may transfer personal data outside of EEA for storage and processing, where 'local laws in non-EEA countries may provide less protection than the laws applicable in the EEA.'</p>	<p>The policy adds that DJI may disclose the information 'if required to do so by law' in response to an 'enforceable request'. It also states that DJI 'may make certain aggregated, de-identified, or non-identifying information about users of DJI Products and Services available to third parties for various purposes, including' 'compliance with various reporting obligations.'</p>
	<p>Hikvision North America's privacy policy covers services for use in conjunction with various Hikvision Internet-connected products. It 'explains how Hikvision handles the collection, storage, and disclosure of information, including personal information.'</p>	<p>Hikvision states that it may transfer personal data to any one of its subsidiaries globally, and that it may also use overseas facilities operated and controlled by Hikvision to process or back up personal information.</p>	<p>The policy adds that the company will not disclose personal information, except in instances in which the company has received prior consent; applicable laws and regulations or authorities require personal information; or the company is protecting its legitimate interests.</p>
	<p>The privacy policy posted on Hikvision.com states that it is applicable to all Hikvision websites. It states that it collects personal information on users based on the type of services they use. Personal information that the company may collect includes IP addresses, visitor volumes,</p>	<p>The policy says Hikvision may transfer personal data to any one of its subsidiaries globally, and that it may also use overseas facilities operated and controlled by Hikvision to process or back up personal information.</p>	<p>It adds that the company will not disclose personal information, except in instances in which the company has received prior consent; applicable laws and regulations or authorities require personal information; or the company is protecting its legitimate interests.</p>

Mapping China's
TECH GIANTS

COMPANY	PRIVACY POLICY PURPOSE	JURISDICTION POLICY	PERSONAL DATA DISCLOSURE
	access times and user preferences.		
	<p>A privacy policy posted on Huawei.com says that it collects personal data depending on how customers interact 'with [Huawei], for example, the website you visit or the products and services that you use.'</p>	<p>Personal data collected by Huawei may be 'processed or accessed in the country/region where you use our products and services or in other countries/regions where Huawei or its affiliates, subsidiaries, service providers or business partners have a presence.'</p>	<p>Huawei may also disclose personal data, 'when it is in connection with an investigation of suspected or actual illegal activity'.</p>
	<p>The privacy policy iFlytek.com applies to iFLYTEK websites. It states that by visiting the Website or using its services, the user agrees that it may collect, use and share [the user's] information in accordance with the Policy.</p>	<p>iFLYTEK may transfer personal data 'to the countries to the countries where you visit the Website where iFLYTEK and its affiliates have a presence' and 'these jurisdictions may have different data protection laws.'</p>	<p>The policy says that the company will disclose personal data in circumstances including 'when, in accordance with the provisions of laws and administrative regulations, the competent authorities shall request it,' 'in case of emergency, to protect the personal or public safety of persons affiliated with the Company, or of the users of this website' or 'in other special or emergency situations.'</p>
	<p>The privacy policy posted to Inspur's website states that personal data will be submitted directly to the company when a customer uses its website, products or services. The data Inspur collects primarily serves the function of the services that the company offers.</p>	<p>The policy states that 'personal data that it collects can be stored and processed in any country where Inspur or its affiliates, subsidiaries or service partners are located. Inspur's primary data centre is located in China, where the policy states Inspur has strict data security protection to avoid the risk of data leakage.'</p>	<p>It adds that Inspur may 'disclose your personal data to relevant law enforcement agencies or other government agencies' and 'in the presence of reasonable request.'</p>

COMPANY	PRIVACY POLICY PURPOSE	JURISDICTION POLICY	PERSONAL DATA DISCLOSURE
	<p>The privacy policy posted to Megvii's English website seems to be written for a PRC audience and it is unclear if this policy is meant to be a global policy. The policy states that it 'only applies to Megvii, and is completely independent of the privacy policy or similar legal texts that our Clients or any third parties may or need to show or provide to you.'</p>	<p>The policy states that 'due to the requirements of Chinese laws and regulations, in principle, the personal information we collect and generate in China will be stored within the territorial scope of China.'</p>	<p>If it is really necessary to transfer your personal information globally, we will transfer your personal information under the premise of complying with the mandatory rules and requirements of China and other relevant jurisdictions (including but not limited to the requirements for the security assessment of exporting personal information from China).' The policy says that Megvii discloses personal data for 'lawful, legitimate, necessary, specific and clear purposes.'</p>
	<p>Meiya Pico's cloud services privacy policy states that the company collects device-related information, including the device models, operating systems and IP addresses of people who use its services. The company collects details of their usage and saves them as logs, including log-in times, access to the network, usage time and more.</p>	<p>It states that the personal information collected and generated by Meiya Pico in the PRC will be stored in the PRC. The company states that it won't store personal information for longer than the time limit specified by relevant laws and regulations, although the privacy policy doesn't mention the time limit or the particular laws and regulations.</p>	<p>The privacy policy states that there are several exceptions for which the company isn't required to seek the user's consent before using, sharing, transferring or publicly disclosing personal information. Those circumstances include instances related to national security and national defence security; public safety and public health; or criminal investigations, prosecution and trials.</p>
	<p>The privacy policy published on Nuctech's website appears to be a global policy and describes company policy on personal information provided to the company when a user accesses 'any website operated by [Nuctech]' or uses the company's 'products and</p>	<p>It says that 'In some countries, including China, countries in the European Economic Area (EEA) and US, this information may be considered personal information under applicable data protection laws.' The policy says user data is 'rarely' transferred across borders to</p>	<p>The policy adds that Nuctech shares personal information with subjects including 'competent law enforcement body, regulatory, government agency, court or other third party, only for the reasons of (i) as a matter of applicable law or regulation.'</p>



Mapping China's
TECH GIANTS

COMPANY	PRIVACY POLICY PURPOSE	JURISDICTION POLICY	PERSONAL DATA DISCLOSURE
	<p>services', or when a user 'otherwise need[s] to provide' their 'personal information' to the company. It states that when users visit its website, the company 'may collect certain information automatically from [a user's] device', such as the user's 'IP address, MAC address, device type, broad geographic location and other technical information'.</p>	<p>jurisdictions where the user is not resident, but in some cases data may be transferred, stored and processed in other jurisdictions where they are not resident. It adds that 'These countries or regions may apply different data protection laws, but we will comply with the data protection laws of relevant countries or regions.'</p>	
	<p>Ping An's privacy policy covering the use of its website (group.pingan.com) provides an explanation of how it collects, uses, and discloses personal information.</p>	<p>It states that the company is established in China and continues to operate servers in China and in other jurisdictions around the world, and that 'the server on which [a user's] personal information is stored may not be in your jurisdiction. [Users] should be aware that the counties in which [their] data is stored may not have data protection laws equivalent to those in [their] country of residence.'</p>	<p>Ping An's privacy policy states that personal information that it collects, directly or automatically, can be used for 'national security, and national defense security purposes'.</p>
	<p>The privacy policy posted to SenseTime's website states that it 'sets out the principles we adhere to and security protection measures we adopt when we provide products or services and process your personal data.'</p>	<p>The policy warns that 'it may be necessary to transfer [a user's] data to a country outside of the country where it was originally collected or outside of [the user's] country of residence or nationality. It will transfer personal data if it's 'in accordance with the applicable laws, requirements of legal procedures, mandatory administrative or judicial requirements.'</p>	<p>It says that SenseTime may 'publicly disclose [a user's] personal data as required by laws, under legal procedures, in lawsuits or upon compulsory requirements of competent authorities under the government.'</p>

Mapping China's
TECH GIANTS

COMPANY	PRIVACY POLICY PURPOSE	JURISDICTION POLICY	PERSONAL DATA DISCLOSURE
	<p>The Tencent privacy policy posted to qq.com pertains to the information it collects, how it uses the information, and user's rights. It is applicable to Tencent services.</p>	<p>The policy explains that Tencent might share personal data with third-party business partners that 'may not be located in your jurisdiction.'</p>	<p>It says Tencent may disclose personal information under circumstances including 'to comply with the applicable laws and regulations' and 'to comply with the requirements of relevant government agencies or other relevant legally authoritative entities.'</p>
	<p>The privacy policy posted to Uniview.com covers the use of the company's products and services. It informs users how their information is collected, used, shared, stored, and protected.</p>	<p>The policy states that 'in order to comply with local laws and regulations, and to bring you with better customer experience and service quality, Uniview Technologies will transfer your personal information to other Uniview Technologies entities around the world. Whenever we are sharing information, especially when we are transferring personal information to countries outside the EU, we will make sure that information is transferred in accordance with this Privacy Policy.'</p>	<p>The policy adds that Uniview has the right to share customers' personal information without consent under circumstances that are related to national security, national defence security, public security or significant public interests.</p>
	<p>WuXi AppTec's privacy policy, which covers visitors when they 'interact with the content, products and services' on the company website.</p>	<p>It states that the company is located in China, and that therefore personal information may be transferred there or to third parties outside of China. Among the reasons for the company to retain personal information are mandatory data retention laws and government orders to preserve data relevant to an investigation. The policy states that for transfers outside of the EEA/UK: WuXi</p>	<p>The policy states that WuXi AppTec shares personal data with various third parties, including 'Competent authorities, courts, third-parties, and bodies in response to a court order, summons or subpoena, lawful discovery requests, regulatory requests, or as permitted or required by law.'</p>

Mapping China's
TECH GIANTS

COMPANY	PRIVACY POLICY PURPOSE	JURISDICTION POLICY	PERSONAL DATA DISCLOSURE
		<p>App Tec 'is located in China, so personal information you submit via our Site may be transferred to China. By providing us with your personal information, you consent to this transfer to China, which your country may not consider to provide for adequate privacy protections.'</p>	
	<p>YITU's website privacy policy 'applies to all products and services offered on YITU's official website (www.yitutech.com) and other products using this privacy policy, including YITU Speech, Business Consulting on the website, and Join Us webpage.'</p>	<p>YITU claims that it will not share its customers' information with any company, organisation or individual outside of YITU's affiliates, except in circumstances in which the company has previously received a customer's consent, in circumstances that require YITU to share information with authorised partners (including courier service providers and infrastructure cloud services), or in cases in which sharing the information is required by law.</p>	<p>The policy says YITU will disclose personal information under circumstances include 'disclosing to third parties, administrations, or law enforcement agencies pursuant to applicable laws or regulations or under the order of administration or law enforcement agency; However, if complied with the law, YITU warrants that it will require the requesting party to issue legal files.'</p>
	<p>According to the privacy policy posted to ZTE's global website, the company may collect and use personal data when customers 'use [their] products and/or services.'</p>	<p>ZTE 'may also transfer your personal data to other countries or regions that may have different laws on the protection of personal data.' Personal data may also be retained 'in a place outside your country, depending on the location of our data center.'</p>	<p>ZTE may collect and use personal data without obtaining your prior consent if, 'the case is directly related to national security and national defense security' or 'directly related to public safety, public health, and major public interests.'</p>