Protecting EU citizens' personal data in China

Zhao, Bo; Mifsud Bonnici, Jeanne

Published in:
International Journal of Law and Information Technology

DOI:
10.1093/ijlit/eaw001

Publication date:
2016

International Journal of Law and Information Technology, 2016, 24, 128–150
doi: 10.1093/ijlit/eaw001
Advance Access Publication Date: 25 March 2016
Article

OXFORD

Protecting EU citizens' personal data in China: a reality or a fantasy?

Bo Zhao* and G.P. (Jeanne) Mifsud Bonnici†

ABSTRACT

With the rise of China's economy and the fast globalization of China's IT industry, an increasing number of EU citizens' personal data are collected and processed on Chinese territory. This article aims to discuss to what extent EU citizens' personal data can be protected under the Chinese and EU data protection frameworks, what are the major problems with the present circumstances, and in which ways EU citizens' personal data cam be better protected as future police choice? To provide a general background, Section II briefly discusses foreigners' legal status and the data protection framework in China. Section III analyses in much detail four practical circumstances under which EU citizens' personal data are processed in China and the possible legal remedies available in case of potential data breaches. Section IV further explains the current situations of judicial mutual assistance between China and EU countries on civil, commercial and criminal matters, in particular regarding the recognition and enforcement of foreign judgments and arbitration awards. The paper is concluded with some concrete suggestions for both Chinese and EU law and policy makers to consider for improvement in their future work.

KEYWORDS: Personal data protection, EU citizens, Chinese data protection law, cross-border data transfer, conflict of jurisdictions

INTRODUCTION

While European Union (EU) citizens enjoy comparatively strong protection of personal data within the EU, EU's data protection legal framework is rather weak when cross-border data transfers and conflict of jurisdictions and laws are at stake.[1] The weak exterritorial protection is plainly seen, for instance, in the recent EU–US data transfers showcased by Snowden's revelation of the mass surveillance, the non-

* Research fellow, Faculty of Law, University of Groningen, the Netherlands.
† Professor of European Technology and Human Rights, Faculty of Law, University of Groningen, the Netherlands.

1 Following European Data Protection Supervisor's approach, in this article data transfer implies the following elements including communication, disclosure or otherwise making available of personal data, conducted with the knowledge or intention of a sender that the recipient(s) will have access to it. See 'The Transfer of Personal Data to Third Countries and International Organisations by EU Institutions and Bodies' (EDPS (European Data Protection Supervisor) 2015) 7 <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf.> accessed 13 February 2015.

effective Safe Harbour programme[2] and the recent findings of EU–US Working Group on Data Protection.[3] While the focal attention in Europe has been largely on how to better protect EU citizens' personal data transferred to the USA, data transfers to other big market players have been largely neglected. This is especially the case when taking into account the large quantity of data flow between the EU and China in recent years resulting from the intensifying economic, political, cultural and educational exchanges.[4]

One may recall the following life realities in which large amount EU citizens' personal data are processed in China: EU citizens' purchase and use of Chinese technical devices such as Huawei's smart phones, tablets and routers; their use of Chinese software, apps, VOIP services and social networking programmes on laptops, smart phones and tablets; their use of Chinese search engines, cloud computing services and security services within and outside China; their use of Chinese online purchase services and banking services; their engagement in various tourist activities such as hotel and flight booking, purchase of train tickets, etc.; their fulfilling registration duties while working or studying in China for a longer period; and other registration or exchange of personal data in China such as passenger names and related personal information. These daily practices involve not only a large population of Chinese–Europeans but also more and more native Europeans who engage with China on various aspects of life and work.

At this moment, however, it seems that no due attention either at the EU level or at Member State level has been paid to the protection of such data transferred and processed in China.[5] A review of current literature does not provide any expected answer to what really happens to EU citizens' personal data processed on Chinese territory. It remains mostly unclear, given no political seasoning smeared, to what extent EU citizens' data privacy is protected under the present Chinese legal framework, and what kinds of legal remedies they may have in case of data breach in China. Most interestingly, neither has there been a single real case reported concerning to date nor any known research has tried to clarify the darkness from either the Chinese or the EU perspective.[6]

Eventually, when one may wonder why silence is the default answer at this point, it is in any sense meaningful to bring up this issue for public attention and to take the initiative to provide some useful information on this non-trivial issue. This is the case

2 And its invalidation consequent to the recent ECJ *Schrems* judgment. Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*.

3 European Commission, 'Restoring Trust in EU-US Data Flows: MEMO/13/1059 27/11/2013' <http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm> accessed 2 October 2014.

4 In this article, China refers only to mainland China, but excludes Taiwan, Hong Kong and Macau with their special laws governing data protection.

5 The same happens on the US side. But the FTC (Federal Trade Commission) recently has un-precedently warned a China-based company of the violation of the Children's Online Privacy Protection Act (COPPA) Rule regarding its collection of precise geo-location information and transition 'to third parties, including advertising networks and/or analytics companies' <http://www.insideprivacy.com/childrens-privacy/ftc-warns-foreign-mobile-app-developer-to-comply-with-coppa/> accessed 11 November 2015.

6 Most scholars researching Chinese data (privacy) protection laws have not addressed this aspect of data privacy law, including Prof Graham Greenleaf who has provided systematic treatment of the Chinese data privacy protection law. Among other works, see for instance Graham Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (1st edn, OUP 2014) 192–225.

especially in view of the deepening EU–China political, economic and diplomatic relationships in every aspect in the long run for which more data of EU citizens' will be collected and processed in China. This research also makes sense by sketching out a real scenario to test the expansive territorial scope of Article 3 of EU's newly proposed General Data Protection Regulation, trying to observe whether it may or may not work in the Chinese context and what shall be done to fulfil that broad promise.[7]

This article first aims to discuss in reality to what extent EU citizens' personal data can be protected under the Chinese data protection framework, what are the major problems of the present circumstances, and in which ways can EU citizens' personal data be better protected as future policy choice? In order not to further complicate the issue, personal data protection in law enforcement sector will not be discussed, although it deserves no less attention, especially when blended with intelligence and security services. Another important aim is to showcase the fact that the exterritorial protection promised under the EU data protection mechanism mainly under Article 4 of the EU Data Protection Directive may not work in practice at least concerning China and needs further substantial legal instruments for support, including, for instance, bilateral treaties and agreements regarding mutual judicial assistance, to keep the promise in reality. To achieve these ends, the article approaches the issue from an individual EU citizen's point of view, reviewing under the present data privacy protection mechanisms of both China and the EU, to what extent one's data privacy can be protected and which legal remedies one can have access to in reality. Or, in a lawyer's approach, it will present an overall picture of the legal avenues a future client may confront under the present legal realities of both Chinese and EU data protection laws.

This article is structured in the following way. To provide a general background, Section 'Personal data protection in China' will briefly discuss foreigners' legal status and the data protection framework in China. Section 'Legal protection of foreigners' personal data in China' will analyse in much detail four practical circumstances under which EU citizens' personal data are processed in China and the possible legal remedies available to them in case of data breaches. Section 'Mutual judicial assistance and law enforcement' will further explain the circumstances of judicial mutual assistance between China and EU countries on civil, commercial and criminal matters, in particular regarding the recognition and enforcement of foreign judgments and arbitral awards. The article concludes with some recommendations for EU law and policy makers to strengthen the protection of EU citizens' personal data in China in their future work.

7 Following the EU Parliament's revision, the Regulation will apply to all processing of personal data by a business operating in the EU market, such as offering goods or services or monitoring of individuals, whether or not the business is physically based in the EU; and it also applies to all data controllers and all data processors established in the EU, whether or not the processing takes place in the EU', which will cover most circumstances of the data processing in China that are to be analysed in Section 'Legal protection of foreigners' personal data in China'. See Progress on EU data protection reform now irreversible following European Parliament vote (14 March 2014) <http://europa.eu/rapid/press-release_MEMO-14-186_nl.htm> accessed 18 February 2016.

PERSONAL DATA PROTECTION IN CHINA

General legal status of foreigners in China

On the whole, EU citizens can enjoy rights to personal data protection and litigation equal to Chinese citizens. Article 32 of the Chinese Constitution protects the lawful rights and interests of foreigners within the Chinese territory.[8] Article 8 of China's General Principles of Civil Law (GPCL) prescribes that its regulations equally apply to foreign nationals as to Chinese nationals.[9] Article 5 of the Civil Procedure Law (CiPL) grants foreign nationals equal litigation rights with Chinese citizens; but in case a foreign citizen's home state imposes restrictions on the civil litigation rights of Chinese nationals, the reciprocity principle applies; and Article 8 guarantees the equal treatment of parties of civil proceedings.[10] Article 395 of the Supreme Court's Interpretation of Criminal Procedure Law (CPL) recognizes foreign parties' litigation rights under Chinese law.[11] In reality, a foreign citizen's equal judicial protection and litigation rights are more substantially guaranteed by international treaties on mutual judicial assistance over civil, commercial and criminal issues between his home state and China.[12]

Development of Chinese data protection law

From 2000 onwards, China has made considerable efforts to enhance data protection by promulgating new laws and updating old laws to meet the challenges of the information economy, which is regarded as the new driving engine of China's future economic growth. Unlike Europe, China does not have a comprehensive data protection law. But to date, there are plenty of laws, regulations and policies covering the major social sectors processing personal data, including postal and transportation services, banking services, E-commerce, juvenile protection, public service sector, telecommunications services, etc.[13] According to a recent study, there are 29 Chinese laws and regulations identified merely in public service sector,[14] not mentioning the private sector.

8 'Constitution of the People's Republic of China (2004 Amendment)' <http://www.lawinfochina.com/display.aspx?id=3437&lib=law&SearchKeyword=constitution&SearchCKeyword=> accessed 8 October 2014.

9 General Principles of the Civil Law of the People's Republic of China (2009 Amendment) 2012.

10 'Zhonghuarenmingongheguo Minshisusongfa (2007 Xiuzheng) (中华人民共和国民事诉讼法(2007修正)) [Civil Procedure Law of the People's Republic of China (2007 Amendment)]' (promulgated by the Standing Comm. Nat'l People's Cong., 28 October 2007, Effective 4 September 1991) (China).

11 Interpretations of the Supreme People's Court on the Application of the 'Criminal Procedure Law of the People's Republic of China' (最高人民法院关于适用《中华人民共和国刑事诉讼法》的解释) 2013.

12 This will be further discussed in Section 'Mutual judicial assistance and law enforcement'.

13 In Greenleaf's words, China has made considerable advances towards the EU victim may gation, defendant)ice of law (Art.cle ions, d by change of texts such as CiPL and CPL. present stage the rule of law in both the public and private sectors regarding data privacy protection, and the cumulative effect of these laws leads to increasing consistency and the inclusion of most minimum privacy principles. Greenleaf (n 6) 225.

14 An Xiao-Mi, Bai Wen-Lin and Sun Shu-Yang, *Legal Requirements for Effective Personal Information Protection through Information Resources Management for Chinese Public Services* (Atlantis Press 2014) <http://www.atlantis-press.com/php/paper-details.php?id=11789> accessed 8 October 2014.

The major legal and policy documents include: Telecommunications Regulations (2000), Administrative Measures on Internet Information Services (2000), Decisions of the Standing Committee of the National People's Congress on Preserving Computer Network Security (2000), Tort Liability Law (2010), Certain Regulations on Standardizing the Order of the Internet Information Service Market (Ministry of Industry and Information Technology, MIIT 2012), Decision on Strengthening the Protection of Network Information (Standing Committee of National People's Congress 2012, as the baseline law), Information Security Technology: Guidelines for Personal Information Protection within Public and Commercial Services (2013; non-compulsory guideline),[15] Telephone User Real Identity Information Registration Regulations (2013), Provisions on the Protection of Personal Information of Telecommunications and Internet Users (2013 MIIT), Consumer Rights and Interests Protection Law (Amended, 2014) and Measures for the Administration of Online Transactions (2013).[16] There are also other data or privacy protection clauses scattered in different regulations and policies in non-IT sectors that govern the processing of personal data essentially for their respective functionalities.

Personal data (information) is defined in China as 'personal electronic information' (literal translation) that 'identifies a citizen and involves a citizen's privacy' by the 'Decision on Strengthening the Protection of Network Information'.[17] In other contexts, similar to EU law, it is defined as 'computer data that may be processed by an information system, relating to a certain natural person, and that may be used solely or along with other information to identify such a natural person' or 'users' personal information', 'information that is relevant to users and can serve to identify users solely or in combination with other information'.[18]

Most related, 'Provisions on the Protection of Personal Information of Telecommunications and Internet Users' prescribes the legal duties and concrete measures of Telecommunication Service Providers and Internet Service Providers to protect users' data security and safety. Like in Europe, it sets out requirements of transparency in data processing, data subjects' consent, full acknowledgement of the users of data processing related issues, data accuracy, sufficiency in data collecting, purpose legitimacy, data confidentiality, data safety and deletion of data after the

15 Classifying personal information into sensitive personal information and general personal information, of which the former, if disclosed or altered, will have adverse impact on data subjects such as identity card numbers, race, political viewpoint, religion or biometric information.

16 For a discussion of personal data protection law in China, see Bo Zhao, 'Personal Data Protection and Regulation in China: the New Challenges' <http://reggov2014.ibei.org/bcn-14-papers/73-96.pdf.>

17 'Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection' (28 December 2012) <http://app.westlawchina.com/maf/china/app/document?&src=nr&docguid=i3cf76ad30000013be0b6b28b5210a151&lang=bi&crumb-action=append&crumb-label=Document> accessed 20 October 2014.

18 Scott Livingston, 'China Releases National Standard for Personal Information Collected Over Information Systems; Industry Self-Regulatory Organization Established | Inside Privacy' (25 January 2013) <http://www.insideprivacy.com/international/china/china-releases-national-standard-for-personal-information-collected-over-information-systems-industr/> accessed 8 October 2014.

consented use. Article 14 prescribes the duty of notification and timely remedy in case of data breach of service providers.[19]

'Tort Liability law' protects civil rights and interests including the rights to name, reputation, honour, self-image, privacy, copyright, patent right, trademarks (Article 2). Patients' 'privacy data' or 'medical history data' are especially protected under Article 62 which requires consent for data disclosure. Article 36 prescribes the tort liability when Internet users or ISPs (Internet Service Providers) infringe others' civil rights or interests by means of networks. Victims are entitled to notify the service providers to take necessary measures including blocking, deletion or disconnection; failing to take necessary and timely measures upon notice, service providers share joint and several liabilities for the additional infringement. Also whilst acknowledging such harm but taking no necessary measures, network service providers shall bear joint and several liability.[20]

Article 252 of the 'Criminal Law' (Amendment 2009, hereafter CL) punishes those who unlawfully open or conceal letters of others thus infringing upon their right to freedom of correspondence.[21] Article 253 criminalizes activities of selling and illegal acquiring and providing personal data by persons working at state organs or key institutions of finance, telecommunications, etc. and responsible for processing personal data, upon incurred serious harms. Article 283 forbids and punishes any illegal producing, selling and using of spy apparatus for wiretapping or photographing secretly. Article 286 punishes anyone who illegally 'conducts operations of deletion, amendment or addition towards data or application programmes which are stored, disposed of or transmitted in a computer information system'.

China's 'Consumer Rights and Interests Protection Law' was amended in 2013, extending protection of consumer personal information from offline to online consuming activities. Article 14 grants general protection of personal information, Article 29 lists nine requirements of personal data processing to improve transparency and accountability of data controllers, Article 39 lays out ways for remedies, Article 50 prescribes civil liabilities for violating such requirements, and Article 56(9) lists administrative responsibilities in addition to civil responsibility to personal information violation, such as being subject to a warning, a fine, confiscation, etc.[22]

'Administrative Measures for Online Trading' sets out regulations governing personal information protection regarding online commercial activities. Article 18 prescribes the principles of legitimacy, properness and necessity, transparency requirements for the purposes, means and scopes of information collection and information use and the requirement of consumer consent in such activities; data

19 'Provisions on Protecting the Personal Information of Telecommunications and Internet Users' (16 July 2013) <http://app.westlawchina.com/maf/china/app/document?&src=nr&docguid=i3cf76ad10000013ff65f15ce3fb28048&lang=en> accessed 20 October 2014.

20 'Tort Law of the People's Republic of China_中国诉讼法律网' <http://www.procedurallaw.cn/english/law/201001/t20100110_300173.html> accessed 8 October 2014.

21 'Amendment to the Criminal Law of the People's Republic of China_中国诉讼法律网' <http://www.procedurallaw.cn/english/law/200903/t20090309_190307.html> accessed 8 October 2014.

22 See Graham Greenleaf and George Tian, *Data Protection Widened by China's Consumer Law Changes* (Social Science Research Network 2014) SSRN Scholarly Paper ID 2404866 <http://papers.ssrn.com/abstract=2404866> accessed 8 October 2014. These articles can theoretically grant foreigners equal means to protect and remedy their data privacy rights.

collection and use (by online dealers) of consumers and other dealers shall publicize their own policies and rules, and shall not be carried in ways against laws and mutual agreement. It forbids disclosure, sale and provision of personal data and business secrecy by data controllers, obligating them to take necessary technical and other measures to secure collected information, preventing their disclosure and data lost, and demanding necessary remedial steps to be taken upon data breach.[23]

On the 9 October 2014, the SPC (Supreme People's Court) issued 'Regulation on Several Issues regarding Application of law in Civil Cases of Violating Personal Rights via Information Networks' (hereafter the October 2014 SPC interpretation), illustrating in full detail how related laws apply in cases regarding violation of rights to names, entitlement, reputation, honour, likeness, privacy, etc. by information networks.[24] It clarifies many controversial issues in application of Civil Law, Tort Liability Law and the 'Decision on Strengthening the Protection of Information Networks' issued by National People's Congress. It covers six major issues, namely: choice of jurisdiction and procedural issues, the meaning of 'acknowledgment of tort activities' of service providers, criteria of recognition of liability and the extent of such liability in reproducing and copying information, scope of personal data protection, liability of illegal deletion and manipulated comments for payment and ways to enhance the protection of tort victims (with emotional damages defined and a maximum damages up to about 62,000 euros). Article 12 forbids network users and service providers to publicize natural persons' private information and other information, including their genetic data, medical data, health profiles, criminal records, home addresses, private activities, etc. It calls upon Chinese courts to support victims' complaints in respect of any damages thus incurred.

This is followed by a new regulation called Measures for Punishment of Conduct Infringing the Rights and Interests of Consumers issued by the Chinese State Administration for Industry and Commerce in January 2016 (to be validated in March). Article 11 for the first time defines consumers' personal information as:

> The information provided by consumer to business operators regarding provision of services or products, including consumers' names, gender, vacation, date of birth, ID numbers, address, contact detail, income and revenue, health condition, consumption circumstances etc., that can singly or in combination with other information be used to identify consumers.

This article also lists three categories of activities that are treated as infringing consumers' personal information.[25]

23 'Administrative Measures for Online Trading' <http://www.lawinfochina.com/display.aspx?id=16309&lib=law&SearchKeyword=&SearchCKeyword=%cd%f8%c2%e7%bd%bb%d2%d7%b9dc%c0%ed%b0%ec%b7%a8> accessed 9 October 2014.

24 'Regulation on Several Issues Regarding Application of Law in Civil Cases Violating Personal Rights via Information Networks of Supreme People's Court (最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定)' <http://www.legaldaily.com.cn/index_article/content/2014-10/09/content_5790789.htm?node=6148> accessed 9 October 2014.

25 For a brief English introduction, see Hunton & Williams LLP, 'China's State Administration for Industry and Commerce Publishes Measures Defining Consumer Personal Information: Privacy and Information

Further, self-regulation of information network service providers has to be mentioned since most of them have the so-called business conduct laws have a privacy policy included, ie standards for consumer personal data protection and transparency rules in data processing. Besides, like in the EU, service providers' terms of uses usually contain a default consumer agreement for data processing as a pre-condition for providing services. Such terms of uses and privacy policy may play a significant role in dispute resolution of future data breaches regarding choice of law and choice of forum.

Lastly, one has to pay attention to various administrative measures set out by different administrative regulations preventing and punishing data breach or providing guidance for law implementation. They include, for example, administrative warnings, fines, public notification, confiscation of illegal gains, revoking licenses or cancelling record-filing or shutting down service, etc.[26] Without a comprehensive data protection law, China's data protection framework consists of, besides the main legal documents above mentioned, a large bulk of administrative regulations and policies scattered in different regulated sectors, most of which have been recently updated to accommodate the Internet Age. Besides, unlike the EU, China has no overarching data protection supervising authority or overseeing body such as European Data Protection Authorities or Data Protection Supervisor (EDPS). Data protection lies in the hands of multiple state authorities that all regulate and govern in their own responsible sectors, but not necessarily with the expected results.[27] The allocation of competence may not always be clear or effective.

Legal protection of foreigners' personal data in china

The above introduced the equal legal status of EU citizens regarding data protection in China and briefly reviewed China's data protection framework. However, it remains largely unknown to EU citizens under which specific circumstances such data protection rights can be violated when their personal data are processed in China for various reasons, and what kinds of legal remedies they are entitled to. To clarify the situation, four circumstances of personal data protection violations and the related legal remedies are analysed in the following. The analysis is predominantly a theoretical one. In reality, there has not been even one case reported yet as of today.

Data processed merely in China

More and more EU citizens visit and stay in China for a wide variety of purposes, e.g. education, temporary employment, sightseeing, business activities and family reunion. During every visit, EU citizens' personal data are processed in China,

Security Law BlogPrivacy and Information Security Law Blog' <https://www.huntonprivacyblog.com/2015/01/articles/chinas-state-administration-industry-commerce-publishes-measures-defining-consumer-personal-information/#more-6788> accessed 9 February 2015. For Chinese text of the legislation, please see《侵害消费者权益行为处罚办法》.

26 As seen in art 11 of Decisions on Strengthening Network Information Protection and art 23 of Provisions on Protecting the Personal Information of Telecommunications and Internet Users. See nn 13 and 15, above.

27 This is well expressed by the Chinese proverb '九龙治水' (nine dragons are all in charge), illustrating that when many bosses are all responsible, in reality no one is really accountable. This is a classical governance dilemma that is popularly observed, for instance, in China's infamous food security and water pollution problems.

including registration for residential and commercial purposes, Internet surfing, using cloud services and software, online purchases, medical treatment, flight and train tickets booking, hotel reservation, etc. What happens if an EU citizen finds that there has been a breach in the safety of his personal data, causing monetary loss or emotional damages?

First, serious violation of personal data interests is punished by Chinese Criminal Law (CL). Article 204 of the CPL grants a crime victim the right to sue, as a self-prosecutor, before a Chinese court. Article 252 protects free correspondence in that anyone who illegally opens another's letters will be punished. Article 253 punishes the sale of personal data or illegal provision by any staff of a state body, or any institutions in finance, telecommunication, transportation, education or health care, etc., as obtained whilst their performing such professional duties or providing services and causing serious consequences; and stealing and acquiring personal information by illegal means with serious consequences are also to be punished; organizations committed any of the above crimes will be prosecuted and punished with a fine, as well as the related persons in charge or responsible for such criminal offences.[28]

EU victims can sue at the primary level of Chinese courts when their legitimate rights are infringed upon by a Chinese citizen but sometimes such cases will be decided by the intermediate courts.[29] Under Article 24 of the CPL, a competent court shall be either at the location of the offence or preferable the residential place of the defendant. They can bring an incidental civil action during criminal proceedings when suffering property losses due to criminal offences (Article 99 of the CPL), which shall be heard together with criminal cases (Article 102 of the CPL). The two crimes under Article 253 of the CL have five years of limitation (with a maximum punishment of five years imprisonment), and the crime under Article 252 of the CL has one year of limitation accordingly (Article 87 of the CL).

They may also resort to national criminal laws of their EU domiciles, because they may only notice such offences while they are back to Europe, or regard this as a better choice, although it would be almost impossible for public prosecutors to investigate such foreign criminal offences in China. Under this circumstance, it depends on whether such data-related offences are criminalized by a Member State in question (dual criminality). If an EU citizen wins the case, according to Article 17 of CPL, the competent Chinese court will decide whether or not to enforce a criminal judgment based on international treaties that China concluded or acceded to, mutual judicial assistance agreements or simply on the principle of reciprocity.

Secondly, 'less serious offenses' upon personal data protection can be remedied under either tort liability or contractual obligation before a competent Chinese court. In many occasions, it is up to a victim which legal approach he may follow on a case-by-case basis. Article 135 of the GPCL prescribes that unless otherwise stipulated by law, the limitation of action shall be two years for application to a people's court to protect civil rights. One may also, upon agreement with the other party, choose

28 Also art 286. See n 17, above.

29 As prescribed by arts 392 and 393 of Interpretations of the Supreme People's Court on the Application of the 'Criminal Procedure Law of the People's Republic of China' (最高人民法院关于适用《中华人民共和国刑事诉讼法》的解释) (n 11).

arbitral proceedings and applicable laws based on explicit expressions (Articles 3 and 18 of the Choice of Law Statute, hereafter CLS).[30]

If EU citizens' personal data interests are violated by Chinese data controllers leading to tort obligation, they can sue at a Chinese court of the habitual residence of a defendant,[31] or one of the place of the offence under Article 28 of the CiPL and Article 2 of the October 2014 SPC interpretation.[32] Regarding applicable law, Article 46 of the CLS prescribes the law of victims' habitual residences as the law governing the infringement via networks or other means of personality rights to privacy, reputation, image and name. Thus, the law of habitual residence, excluding procedural law, will be applied, which naturally leads to the suspect of primary courts' competency to implement foreign laws.

If EU citizens assume that resorting to contractual obligation is a better option, since most contracts with large amount of personal data processed would include privacy clauses, in particular, regarding network services. They can file cases, according to Article 23 of the CiPL, at a competent court of a defendant's domicile, or of the performance place of contractual obligation. Both parties may choose, upon written forms, a governing forum to settle disputes from one of the following places, including a defendant's domicile, performance or signature place of a contract, a plaintiff's domicile or other locations with actual connection with the dispute, provided that the provisions on hierarchical jurisdiction and exclusive jurisdiction are not violated (Article 34 of the CiPL). The choice of forum can also be settled in contractual terms either as free choice of both parties or as mandatory terms incorporated in contracts completed by customers and online commercial operators on third-party E-commerce platforms in China.

The choice of law issue, however, is vague under the CLS in case of disputes over consumer contracts. Article 42 first prescribes that a consumer contract is in general governed by the law of a consumer's habitual residence in general. This means that the related EU law (including national data protection law) shall be applied. However, the second clause of the same article may lead to controversy. It states that 'If the consumer chooses the law of the place where the commodity or the service is provided, or if the business operator *does not engage in any related business activity* at the habitual residence of the consumer, the law of the place where the commodity or service is provided shall be applied.'[33] First, while EU consumers use Chinese services or purchase goods (via the Internet) from China, mostly such contracts will choose Chinese law as the default governing law, and thus Chinese law shall apply. Secondly, however, it is doubtful what does 'where the business operator does not

30 See Trey Childress, 'P.R. China's First Statute on Choice of Law (translated in English)' <http://conflictoflaws.net/2011/p-r-chinas-first-statute-on-choice-of-law-translated-in-english/> accessed 24 October 2014.

31 Recently, habitual residence has been more used than domicile to ascertain the legal relationship between a person and a location in China. See Mo Zhang, 'Codified Choice of Law in China: Rules, Processes and Theoretic Underpinnings' (2012) 37 NCJ Intl L & Com Reg 131, 133.

32 See Regulation on Several Issues Regarding Application of Law in Civil Cases of Violating Personal Rights via Information Networks.

33 Emphasis added.

engage in any business activity in the habitual residence of the consumer' is interpreted in particular in the context of the Internet-based business activities.

If a Chinese business operator has an establishment in Europe, then the law of a consumer's domicile in Europe shall apply. But if no establishment is found as such, it is rather problematic how to define or interpret the wording of 'engage in any business activity'. For example, while using Chinese search engines like Baidu established in China, an EU subscriber may choose to enter into a contract of no compensation nature. But whether or not such business operators 'engage in any related business activity' in the EU is uncertain, when such search services are available to all EU Internet users. If following the reasoning of the most recently proposed General Data Protection Regulation, such services shall be regarded as business activity under Article 3.2 (a),[34] and the related EU law would apply. In this case, a court in an EU Member State may apply EU law (if and when the new Regulation will be in force) and presumably a Chinese Court would not apply the Regulation, but its own conflict of law rules (which is discussed above).

Also if following the analysis of Working Party 29, such search engines can be regarded as having business activity in terms of data collecting, because the use of cookies, JavaScript, ad-banners and spyware on personal computers located in the EU means making use of 'equipment' within the EU by a non-EU website to collect personal data of EU visitors.[35] But if such services available on the EU border would not be regarded as engaging 'in any business activity', then Chinese law shall apply as the law of the place for provision of commodity or service under Chinese law.

The above discussion addressed the situation that an EU litigant may have the choice to sue in China upon finding his rights to personal data protection violated. But how about the circumstance of being unable to seek remedy due to one's short stay in China, or delayed acknowledgement of offence after returning to Europe? In both occasions, one may still initiate an action in China within two years in case of civil offence or prosecute an offender within a period specified by the CL. To initiate litigation at an EU court of one's domicile is also possible. Because a targeted defendant is domiciled in China, this falls out of the scope of the Regulation Brussels I (RBI),[36] but within the jurisdiction of Member States whose respective laws shall apply.

34 'This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union.' See 'EU General Data Protection REgulation (GDPR Consolidated Text)' <https://iapp.org/media/pdf/resource_center/2015_12_15-GDPR_final_outcome_trilogue_consolidated_text.pdf>.

35 Lokke Moerel, 'The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?' (2011) 1 IDPL 28, Section VII. In the Chinese contexts, the term refers to any business activity in original Chinese (任何经营活动) include any business activities besides investment and financing in general.

36 Council Regulation (EC) No 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001R0044> accessed 14 October 2014.

For example, one may sue before a Luxembourg court, since Article 14 of the Luxembourg Civil Code allows any nationals to sue a foreigner before a Luxembourg court for execution of a contractual obligation, either in Luxembourg or abroad, even if the person in cause does not reside in Luxembourg.[37] Also one may sue before a Dutch court against a Chinese defendant under Article 6 of the Dutch Civil Procedural Law, either under clause (d) regarding contractual obligation or under clause (e) regarding tort offence.[38] Furthermore, with the recast of the Brussels Regulation coming into force in 2015, residents outside the EU can be sued in courts of EU Member States as identified by Article 6 and Recital 14.

Data collected in China but processed in the EU

EU citizens' personal data can be collected in China and then sent back and forth between Europe and China, consequent to their use of apps, software, social networking programmes, laptops, portable devices and smart phones that were purchased, downloaded or registered in the EU; or the use of email services and cloud services host in the EU; or merely the surfing of EU websites. After such personal data are received, archived, processed or inspected by EU service providers, their personal data will be transferred back to China to EU users during or after the used services. So even if an EU citizen is physically in China, there is a certain period of time during which his personal data are transferred from EU territory to China.

However, to one's big surprise, there is still no specific Chinese law governing the data of either Chinese nationals or foreigners transferred to third countries.[39] But there exists a guiding policy document that was issued by MIIT, though not binding, to restrict the transfer of person data outside China without meeting prescribed conditions.[40] This means that there are no similar, effective legal instruments established to satisfy the requirement of adequate level of protection in Article 25 of the EU Data Protection Directive and the derogation clause in Article 26 governing data transfer to third countries.[41]

37 Luxembourg Law Office, 'Civil Law in Luxembourg' <http://www.lawyers-luxembourg.com/civil-law-in-luxembourg> accessed 12 October 2014.

38 'Code of Civil Procedure (English Version)' (*Dutchcivillaw*) <http://www.dutchcivillaw.com/civilprocedureleg.htm> accessed 12 October 2014.

39 Dong Xiao, 'Data Protection in China: Overview' (June 2014) <http://uk.practicallaw.com/4-519-9017#> accessed 24 October 2014.

40 art 5.4.5 of the Guideline for Personal Information Protection for Information Systems in Public and Commercial Services (信息安全技术 公共及商用服务信息系统个人信息保护指南). Chinese version available at <http://www.miit.gov.cn/n11293472/n11293832/n11293907/n11368223/13590447.html> accessed 24 December 2015.

41 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> accessed 17 February 2016. But this does not mean personal data of Chinese users are not protected from illegal collection on Chinese territory by foreigners. Recently, two foreigners were punished for illegally obtaining private information of Chinese citizens in China for foreign customers. See James T Areddy and Laurie Burkitt, 'China Convicts Two Foreign GSK Investigators' *Wall Street Journal* (8 August 2014) <http://online.wsj.com/articles/china-trial-of-british-american-investigators-begins-1407469079> accessed 15 October 2014.

For simplicity, the circumstance of an EU mobile phone user will be discussed before the analysis of other circumstances. If an EU mobile/smart phone user is taking an EU-contracted phone with him in China, functioning on a roaming agreement between his telecommunication service provider(s) and a Chinese telecommunication company, there are several choices in case of data breaches, although the geographical locations are usually hard to be traced down.

If a data breach incident 'happens within the EU', while he is using the EU-contracted service in China via a roaming agreement, he may choose to protect his personal data in various ways. First of all, under the protection of Articles 22–24 of Directive 95/46/EC and related national data protection laws, one can apply for administrative remedies and judicial remedies as such prescribed at a competent court.[42] Furthermore, he can sue under either contractual obligation or tort liability in an EU court. The best option is to sue in a competent court of the place where the contractual obligation in question is performed, or the place of the defendant's domicile, or of one's own domicile, according to Articles 5.1, 15.1 and 16.1 of the Brussels Regulation. In this context, if there is no choice of law agreement made by both parties to a contract, the applicable law would be the law of the country where the service provider has habitual residence (Article 4 (b) of Rome 1), or of the habitual residence of the consumer in general (Article 6.1 of Rome I).[43] In this case, there is no connection substantial enough to incur the jurisdiction of any Chinese court under both the EU and Chinese law.

The EU citizen can also protect his rights by means of tort law as seen in one's best interest. In this context, he may sue before an EU court of the place where the harmful event occurred or may occur (Article 5.3 of RBI); and the applicable law would be the law of the place of the common domicile of both parties of the complaint (Article 4.2 of Rome II),[44] or of the place in which the damage occurs (Article 4.1 of Rome II), or the place with which the tort or delict is manifestly more closely connected as it is clear from all the circumstances of the case (Article 4.3 of Rome II), or the law of the free choice of the parties of concern (Article 14 of Rome II). In this case, there is no substantial connection with any Chinese court which has no jurisdiction.

If a data breach 'happens within China', one may still sue the involved EU telecommunication service provider in a competent EU court as a contractual dispute as prescribed by the Brussels Regulation, as discussed above. This is because the contractual duty (to protect users' personal data) is mainly performed within the EU, albeit with a data roaming agreement with a Chinese company (as sub-contracting).

42 In this case and other similar cases, DPD 95 will apply and it largely depends on how the Directive is transposed to domestic laws by Member States. In the following, the analysis will be limited to tortious and contractual litigations thus incurred in general at the EU level, instead of checking respective Member State laws.

43 Regulation (EC) 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] <http://eur-lex.europa.eu/legal-content/en/ALL/;ELX_SESSIONID=m1YWJK5hgVJP3yBlBq6GgTBwq1LC13PfRbzpFhQ23dTbkMfDNyT2!1564011092?uri=CELEX:32008R0593> accessed 29 June 2015.

44 'Regulation (EC) No 864/2007 — the Law Applicable to Non-Contractual Obligations (Rome II)' <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32007R0864> accessed 18 December 2015.

The applicable law will be the same as discussed above. But in this context, one may choose to include the Chinese sub-contractor as a joint defendant, if allowed by the applicable national law. The victim can sue in a Chinese court according to Article 23 of the CiPL which grants jurisdiction to the court of the defendant's domicile. According to Article 42 of the CLS, the applicable law shall be the law of the domicile of the consumer when consumer contract is of concern.

One can also protect his personal data interests by filing a tort claim in a competent Chinese court according to Article 28 of the CiPL, which grants jurisdiction to the court of the place where the harmful event happened, or of the defendant's domicile. The applicable law would be the law of the EU citizen's domicile country as prescribed by Article 46 of the CLS. Also one may act as a self-prosecutor before a Chinese court, with the possibility of an incident claim of tort damage, if the data breach has serious consequences and made by such suspects as defined under Articles 252 and 253 of the CL, as discussed in Section A.

In case of an EU 'subscriber' using services of email, cloud computing, software, apps, search engines, or social networking that are host in the EU, but accessing them from Chinese networks (in particular the Internet), the situation is not that different from that of the user of EU mobile phones in China. The major difference is that there is no sub-contracted data roaming guaranteed under bilateral agreements, which means less legal certainty. Under this circumstance, terms of services or privacy policies that are presumed to be known and consented by EU users, may allow justified expectations of data safety protected by EU national data protection laws, including the Directive 95/46/EC, and other consumer protection laws. Of course, EU subscribers can also resort to tort law for protection, if this is in their best interest.

With respect to 'unsubscribed' use of search engines and surfing of web sites host within the EU, an EU user physically in China has to be connected by Chinese networks to access those services. One's personal data can be processed by cookies, JavaScript, ad banners and spyware that are put on the device, whether a Chinese device or an EU one. In this case, the EU user may sue the service providers under tort liability in an EU court at the place 'where the harmful event occurred or may occur' (Article 5.3 of RBI). The applicable laws would be the same as prescribed by Articles 4.1–4.3 or 14 of the Rome II, as discussed in the above mobile phone user case. In this context, there is no substantive connection with Chinese law that is sufficient enough to award jurisdiction to Chinese courts.

Data collected in the EU but processed in China

Compared with the above circumstances, it is a much complicated issue when EU citizens' personal information (data) are collected on EU territory, but processed in China. This may happen: (i) when EU citizens have bought Chinese hardware with pre-installed software including PCs, tablets, smart phones, laptops and routers from China, and use them within the EU; (ii) when they are subscribed users of social networking services, apps downloaded on portable devices, VOIP software, email services, cloud computing services, e-journals, E-commerce services in China or Chinese search engines, but receive services or goods within the EU; or (iii) when as unsubscribed users they download software such as QQ, and 360 safety programmes, or other software on PCs,

and personal devices, but use them within the EU;[45] or (iv) when they are surfing Chinese websites or playing online games that are host within China; and last (v) when they use services or goods provided in the EU, either by EU data controllers or by Chinese data controllers with establishments in the EU, but the collected data are sent to China for processing. For convenience, first circumstances from (i) to (iv) will be analysed together, before proceeding to discussing circumstance (v).

In the circumstances from (i) to (iv), EU users' data will be collected through the use of products and services and processed in China. This includes personal information given by users, information acquired from the use of services, device information, log information, manners of using, IP address, local storage, URL information, Unique Serial Numbers, etc. Such information can be archived, analysed, profiled or handed out to third parties in China like business partners or security agencies, or transferred to third countries, which directly threatens EU citizens' personal data right that is protected by the EU Charter of Fundamental Rights and other related secondary legislations.[46]

The above scenarios are not far-fetched, but well observed in recent events. With the increasing share of Huawei's products on European market including smart phones, tablets and network infrastructure facilities from WLAN routers to fibre optic cables, there is no doubt that personal data of EU customers and consumers are very possibly to be transferred to China.[47] Such data may bear considerable values for both the Chinese intelligence agencies and their NSA (National Security Agency) rival, as well as Chinese business competitors with ambition to land on EU market.[48] Recently, a western user using a smart phone ordered from China found that his background screen was changed to a red Chinese national flag celebrating 'the Chinese National Day', and he could not change it back.[49] This may indicate the potential control effort via preinstalled software by his Chinese producer as such

45 Some of which are now promoting to the International community their products with free service in both English and Chinese, see 360 international at <http://www.360safe.com/> and QQ international (with privacy declaration) at <http://www.tencent.com/en-us/zc/privacypolicy.shtml>

46 For a general discussion of the EU laws protecting personal data, see in general: Morten Kjaerum and Philippe Boillat, *Handbook on European Data Protection Law* (Publications Offices of the European Union 2014) <http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law> accessed 11 October 2014.

47 Now Huawei is the world's second largest network equipment supplier. 'NSA Spied on Chinese Government and Networking Firm Huawei' *Spiegel Online* (22 March 2014) <http://www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html> accessed 15 October 2014.

48 NSA broke into Huawei's headquarter in Shenzhen and acquired access to a large amount of data from the company, claiming 'Many of our targets communicate over Huawei-produced products. We want to make sure that we know how to exploit these products.' See n 47, above. Similarly but in contrast, there are also large scale data breaches of the American citizens supposedly conducted by Chinese hackers reported. See, for instance: Jason Millman, 'Health Care Data Breaches Have Hit 30M Patients and Counting' *The Washington Post* (19 August 2014) <http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/> accessed 4 February 2015.

49 'The Phone I Ordered from China Changed My Background Today . . . Apparently It's National Day (I Can't Change It Back)' (*9GAG*) <http://9gag.com/gag/a8b3oKe> accessed 3 October 2014.

happened to the customers from Taiwan.[50] Also routers made in China but sold elsewhere in the world are found to have back doors allowing the hacking of consumer's PCs or other devices.[51]

In this context, the eminent questions are how can EU citizens' rights to privacy and personal data safety be remedied upon data breach far away in China?[52]

First of all, whether as a matter of tort liability or breach of contractual obligation, since a Chinese defendant does not domiciled in any EU Member State the Brussels Jurisdiction Regulation will not apply, and the defendant 'is in general subject to national rules of jurisdiction applicable in the territory of the Member State of the court seized' according to Recital 9. [53] In this case, the applicable law would be chosen by the private international law of that state. The recognition and enforcement of EU national court verdicts, as well as possible judicial assistance between Member States and Chinese judicial authorities, will be discussed in Section 'Mutual judicial assistance and law enforcement'. The following will analyse possible legal remedies and protection of the plaintiff's right to data protection 'under Chinese law'.

Under circumstance (i), if hardware devices such as smart phones, PCs, tablets and routers are bought from China (in person or via the Internet) and used in the EU via the EU's networks, and 'data breach happens in China', this leads to the following consequences. First, when an EU consumer has registered for services of products maintenance, products promotions, software updates, data analyses or data synchronizing, they actually have completed consumer/service contracts with Chinese counter parties, whether completed in EU or in China after the purchase. In this case, the EU consumer may have a claim to contractual breach before a Chinese court at the domicile of a Chinese defendant or at the place of the performance of the contractual obligation in question (Articles 22 and 24 of the CiPL). The applicable law will in general be the EU Member State law of one's habitual residence, or the law of the place where the commodity or the service is provided will apply upon the agreement of a consumer contract (second section of Article 41 of the CLS). Or the law of the domicile of the Chinese service provider or product producer shall apply to consumer contract disputes, given that they carry out no business activity at the domicile of the EU consumer (Article 42 of CLS). It would usually be the case that Chinese law is chosen as the applicable law for commodity and service contracts.

Of course, the EU citizen is more likely to sue before a national court under Article 4 (1) of Council Regulation (EC) No 44/2001 (Brussels) or under Article 4.1 of the Data Protection Directive EC/95/46. For contract litigation, the applicable law can be the law of the residency of the EU consumer (Article 6.1 of Rome I on

50 Mohit Kumar, 'Xiaomi Phones Secretly Sending Users' Sensitive Data to Chinese Servers' *The Hacker News | Biggest Information Security Channel* (9 August 2014) <http://thehackernews.com/2014/08/xiaomi-phones-secretly-sending-users.html> accessed 15 October 2014.

51 See 'Backdoor Found in Chinese Tenda Wireless Routers, Allows Root Access to Hackers' *The Hacker News | Biggest Information Security Channel* (18 October 2013) <http://thehackernews.com/2013/10/backdoor-found-in-chinese-tenda.html> accessed 16 October 2014.

52 This section will not discuss the circumstance under which EU citizens buy Chinese products and use them within the EU border, but with data breach happens within the EU, which will completely falls under the jurisdiction of the EU law, even if there might be data transferred back to China for processing.

53 See n 36, above.

laws applicable to contractual obligations), or the law previously chosen by parties, or the law of the seller or services provider (in this case the Chinese defendant) given there is no agreement on Choice of law (Article 4 1 (a) and (b) of Rome I). For tort litigation, the EU victim may sue at a national court subject to Article 4 (1) of Brussels I and Article 4.1 of the Data Protective Directive 94 and the applicable law would be the law of the victim's domicile or another country with the closest connection under Article 4 (1) and (2) of the Rome II. But the recognition and enforcement of EU court judgments in favour of the plaintiff remains gloomy under the present circumstances of Chinese law.[54]

When EU users do not register, then the risk of data breach from service providers in China is rather low. But this means that they would not have the necessary update and maintenance from Chinese service providers and hardware producers. Furthermore, it is almost impossible to prevent hardware producers to have certain pre-installed software capable of collecting users' data and transferring them back to product producers in China. In this case, an EU victim may claim under tort obligation before a Chinese court at the place where the harmful event happened or the place of the defendant's domicile (Article 2 of the October 2014 SPC interpretation and Article 29 of the CiPL). The applicable law would be the national law of one's habitual residence in the EU (Article 46 of the CLS).

Under circumstance (ii), subscription (and registration) is a pre-condition for using Chinese social networking programmes like Weibo(Chinese microblog), email services, online game services, cloud computing services, apps and E-commerce services host in China. Users' subscription usually leads to contractual obligation of service and commodity providers in China. In context (iii), when unsubscribed EU users download software such as Tengxun's safety programmes, or 360's security packages on PCs, smart phones or tablets, installation would be conditioned on their informed consent of the privacy policies contained in terms of services or policy clauses, therefore, they also enter into service agreements or contracts with consent. In both (ii) and (iii), their personal data are to be collected and transferred back to China for processing. [55]

In case of data breach in China, similar to the above discussion of the circumstance (i), an EU citizen can file a case at a court at the place of performance of contractual obligation or at defendant's domicile under Article 24 of the CiPL. The applicable law would be the law of one's habitual residence or of the place of provision of service or goods under 42 of the CLS. If an EU user of such services will choose to resort to tort liability, if it is at one's best interest, he or she may initiate an

54 This will be further discussed by Section 'Mutual judicial assistance and law enforcement'.

55 For example, the English version of Service Agreement of 360's Total Security software is based on user's default consent to its privacy policy, which lists users' data to be processed by the company. This includes their log information, device information, URL information, Unique Serial Numbers, information during use of the software in particular scanning, users' using patterns, information about users' computer files, etc. and permits sharing them with third parties <http://360safe.com/privacy.html>. The company has been constantly 'accused' in China for data breach and privacy invasion in recent years. (See 'Privacy Issues With China's Qihoo 360 Technology, Which Provides Free Antivirus Software, Are Becoming More Public; But Qihu Strongly Rebuts Accusations' *International Business Times* (9 April 2013) <http://www.ibtimes.com/privacy-issues-chinas-qihoo-360-technology-which-provides-free-antivirus-software-are-becoming-more> accessed 17 February 2016.)

action before a competent court either at the Chinese defendant's domicile, or at the place of the wrongful act in question under Article 2 of the October 2014 SPC interpretation and Article 29 of the CiPL. The applicable law would be the law of one's EU habitual residence of the victim under Article 46 of the CLS.

Under circumstance (iv), when unsubscribed EU users browse Chinese websites and use Chinese search engines that are host within China, certain categories of personal data such as device information, anonymous identifiers, canvas fingerprints, log information will be collected at their EU devices by means of cookies, JavaScripts, canvas fingerprint, etc. and be processed in China. Such information may not have direct impact on EU users, but when combined with other personal information collected by other means for data profiling, they may lead to data infringement. In case of data breach in China, the best choice for an EU victim is to sue under tort liability before the Chinese court of the domicile of the concerned website host under Article 2 of the October 2014 SPC interpretation and Article 28 of the CiPL. The applicable law would be the law of one's habitual residence of the EU user under Article 46 of the CLS.

Lastly, circumstance (v) is the most common one under which EU citizens' data may be transferred to China for processing. This includes a large variety of cross-border data transferred and processed in China, regarding EU and Chinese flight services, services of EU or Chinese travelling agencies, data processing services outsourced to China, customer services by Chinese producers via their EU co-operators or consumer data collected and sent to mother companies by EU subsidiaries or establishments. The majority are clear cases, because of defendants' physical legal presence in the EU. The plaintiff may merely sue the concerned EU defendants who are responsible for such cross-border data transfers according to the Brussels Regulation; and the applicable law would be decided either under Rome I or Rome II. It could also be the case that since data breach may happen in China, the EU plaintiff may list a Chinese party as a co-defendant for breach of contractual obligation or for tort liability, once this fits the plaintiff's best interest.[56]

Data collected outside the EU and China but processed in China

With the fast development of Internet and Telecommunications technologies and of globalization, it is a daily reality that an EU citizen would stay somewhere else outside both the EU and China, but with his personal data processed in China: whether he is on a business trip in the USA, negotiating with a Chinese client for a cross-border sale contract, or he is visiting Chinese websites or using Chinese search engines to find sub-contractors for an international project, or he is checking Chinese blogs or news portals for academic research, or he is using Chinese social networking programmes to communicate with his friends in China, etc. In such occasions, how could his personal data be protected in case of data breach in China, and what are the legal remedies available?

56 For a practical guide, please refer to: Ivana Kunda and Carlos Manuel Gonçalve de Melo Marinho, *Practical Handbook on European Private International Law* <http://ec.europa.eu/justice/civil/files/practical_handbook_eu_international_law_en.pdf> accessed 17 October 2014.

In general, the most ideal choice for legal remedy is to sue in an EU court of one's domicile or national state if whose law accepts one's complaint against a Chinese defendant, whether under tort liability or under contractual obligation. The applicable law will be decided by the governing national Member State law, unless both parties have otherwise agreed upon the applicable law in service contract, or in afterward negotiation. Of course, the EU citizen may sue in a Chinese court, if this fits one's best interest, as discussed in the above sections.

However, most Chinese companies that are established in China and act as service providers have no foreign clients in minds. They set out privacy policy in terms of services (in Chinese) and choose Chinese law (excluding conflict of law rules) as the applicable law, and the competent court would be a Chinese court of the place of the completion of the contract (usually the company's domicile), when disputes are not settled between two parties.[57]

Furthermore, there is a particular situation for consideration. That is, if an EU citizen has purchased services or commodities from Chinese companies that are domiciled outside both EU and China, such as in the USA, and his personal data or information are sent to China for processing (from a subsidiary company to a parent company). Usually a contract is completed in a third country, or on the company's international (English) website that has the intention to reach foreign customers. In this case, usually the applicable law is prescribed in terms of services.

For example, the terms of services of Qihu's 360 Total Security Software choose the law of the state of New York as the governing law, excluding its conflict of law rules. It requests a settlement between a customer and the company in the first instance, otherwise, such a dispute shall be subject to the American Arbitration Association under the Commercial Arbitration Rules and Supplementary Procedures for Customers; and it excludes class action or a trial by jury.[58] TengXun's QQ international software license agreement states:

> The validity, interpretation, execution, implementation of and the settlement of disputes in relation to the user-service provider agreement shall be governed by the laws of California State, rather than Conflict Law. Interpretation of the agreement and enforced execution should be submitted to the Court having jurisdiction in San Diego, California.[59]

Under the above circumstances, EU citizen as subscribed users would be under the jurisdiction of the US courts with US law applied to data breach disputes. With English as the language of communication and terms of service accessible to EU users, there would be conflict of jurisdictions if an EU user may file a law suit in a competent EU court, under Article 4.1(c) of the DPD, or Article 4 of the Brussels Regulation (recast), or their national laws.

57 As exemplified by the terms of service of QQ's email service(in Chinese) <https://mail.qq.com/egi-bin/redtemplate?check=false&t=mail_clause

58 <http://www.360safe.com/totalsecurity/en/licence.html>

59 <http://zc.qq.com/chs/agreement1_en.html>

MUTUAL JUDICIAL ASSISTANCE AND LAW ENFORCEMENT

Once court verdicts or arbitral awards are issued in EU citizens' favour, they have to be recognized and enforced by competent courts in China. Also during arbitration process and court proceedings, there are needs for mutual assistance between China and the EU in seeking evidence, communications of legal documents to foreign parties, conducting investigation and other litigation actions. Absent mutual law enforcement treaties, China takes the default position of the recognized rule of public international law that no jurisdiction can allow prosecution within its borders under the criminal law of another jurisdiction. And no foreign organ or individuals may serve documents or conduct any investigation and collection of evidence within the Chinese territory, unless approved by capable Chinese authorities and allowed by Chinese law (Article 277 of CiPL).

Regarding criminal offence regarding data privacy breach, Article 17 of the Chinese Criminal Procedure Law prescribed that in accordance with the international treaties which the People's Republic of China has concluded or acceded to or on the principle of reciprocity, the judicial organs foreign countries may request judicial assistance from the Chinese side in criminal affairs.

Regarding civil offences, Articles 281 of the Chinese CiPL prescribes that a foreign judgment creditor of a valid foreign court decision can directly file a petition with a competent Chinese intermediate court for recognition and enforcement of the judgment, or a foreign adjudicating court may make a direct request to a Chinese competent intermediate court for recognition and enforcement according to the treaties of which China has participated and ratified, or the reciprocity principle. Competent Chinese courts may recognize the validity of a foreign court decision and issue an order of enforcement;[60] otherwise, the court may reject such request (Article 282 of the CPL). With regard to awards of foreign arbitration institutions, the concerned parties shall directly make such requests to competent courts of the place where such awards debtors reside or where their properties are located, which shall be in accordance with the international treaties that are participated in and ratified by China, or the principle of reciprocity (Article 283 of the CiPL).

Chinese court and foreign courts may request the service of legal documents, judicial investigation, collection of evidence or other litigation actions based on the international treaties that China has concluded or acceded to (Article 276 of the CPL). Such requests can be made via channels prescribed by related international treaties, or through diplomatic channels, given no such treaties exist between the two sides. Such requests and the annexed documents shall be appended with Chinese versions or the texts in a language specified in the relevant international treaty (Article 278 of the CiPL). Besides, the execution of foreign judicial requests shall follow the procedure of Chinese law; and such requests may be carried out in special ways as demanded, but must not violate any laws of China (Article 279 of the CiPL). Chapter 25 of the CPL prescribes the service and time periods under Chinese law regarding judicial issues. Articles 263–265 prescribe that foreign litigants must have Chinese lawyers to represent their interest in legal proceedings in China,

60 Usually on the conditions that such court decisions are not contrary to the basic principles of Chinese law, and not against Chinese sovereignty, public safety and public and social interests.

and list other related legal requirements for empowering such litigation representatives.

In contrast to the circumstance, when the CiPL was not amended 10 years ago, Chinese courts are now more likely to recognize and enforce foreign judgments.[61] This is also reflected in the increasing number of bilateral treaties on mutual judicial assistances regarding civil, commercial and criminal matters. Nowadays, China has signed such treaties with Italy (civil and criminal), Malta (criminal), Portugal (criminal), Spain (civil, commercial and criminal), France (Criminal), Latvia (criminal), Estonia (criminal), Lithuania (civil and criminal), Romania (civil and criminal), Belgium (civil), Hungary (civil and commercial), Bulgaria (criminal and civil), Greece (civil and criminal) and Poland (civil and commercial).[62] Furthermore, China has ratified the New York Arbitration Convention in 1987 which applies to disputes of contractual and non-contractual commercial relationships in China. Application for enforcement of arbitration awards can be made to an Intermediate People's court of the place of a Chinese party's domicile or residence or of the main administrative body of a Chinese legal entity. Arbitral awards made in the contracting EU Member States to the Convention shall be recognized and enforced in China after reviewing by competent Chinese courts.[63]

However, one shall not expect to have a foreign judgment generally recognized and enforced in China at present days unless they are devoice judgments. As Zhang's empirical research indicated, recognition and enforcement of foreign judgments (except divorce judgments) are hardly possible at present stage, if there have not been China-foreign bilateral treaties concerning mutual judicial assistance.[64] Still provisions of such treaty or agreement are too general and ambiguous, and they differ much from each other in some aspects, not mentioning the fact that many important world powers including the USA, Japan, Germany, the UK and India are not included.[65] It is a matter of fact that 'China has not yet offered a good environment for the recognition of foreign judgment.'[66]

CONCLUSION: TOWARDS A BETTER PROTECTION

The previous sections have analysed the Chinese legal framework that offers legal protection of EU citizens' personal data in case of data breach on Chinese territory and the legal remedies available under the related laws. On the whole, China has been strengthening her data protection framework in the past decade and granted foreigners the equal legal protection with Chinese nationals. But this does not mean

61 Mo Zhang, 'International Civil Litigation in China: A Practical Analysis of the Chinese Judicial System' 25 BC Intl & Comp L Rev 88–89.

62 Data are taken from Westlaw.China and available from the author upon request.

63 See 'Notice of the Supreme People's Court on Implementation of the Convention on the Recognition and Enforcement of Foreign Arbitration Awards Acceded to by China' (March 1987) <http://app.westlawchina.com/maf/china/app/document?&src=nr&docguid=i3cf76ad30000011ef347f17f6335fbaa&lang=bi&crumb-action=append&crumb-label=%E6%96%87%E4%BB%B6> accessed 20 October 2014.

64 Wenliang Zhang, *Recognition and Enforcement of Foreign Judgments in China: Rules, Practice and Strategies* (Kluwer Law International 2014) 329–30.

65 Ibid 339–40.

66 Ibid 342.

that it naturally satisfies the requirement of adequate level of protection under Article 25 of Directive 95/46/EC, in particular in view of China's law enforcement problem, popular law breaches and the likely window dressing Binding Corporate Rules. For compliance with the EU data export rules, of course Model Contracts are one option (not further explored in this article).

Theoretically, there are legal remedies available to EU citizens when their data are processed in China, whether they may sue directly in China or from their EU domiciles. But as far as the present literatures illustrate, yet there is still not a single case reported regarding data privacy invasions of EU citizens. This definitely will not be the case in the long run, if taking into account of the escalating data transfers and exchanges between EU and China, consequent to the escalating economic, political, educational and cultural exchanges.

On the EU side, too much attention has been paid to the protection of EU citizens' data safety in the USA after Snowden's revelation. However, it remains 'largely' unclear what has happened to EU citizens' data transferred and processed in China.[67] Though it is obvious the intention of the EU data protection laws to claim exterritorial jurisdiction almost over the whole Internet by means of establishing more connections with EU courts, the following issues need further clarification regarding China. Firstly, whether the status quo of no complaint of data breach in China means no such breach exists, or the damages are too trivial to be taken care of, or the legal remedy costs are too high to bear by EU victims? If the latter is the case, maybe certain positive measures shall be taken for assistance. Secondly, it is not clear if EU victims may have equal legal remedies across the EU in case of data breach in China, because such a matter falls out of the scope of the Brussels Regulation (with the defendant being a Chinese domicile), but into the hands of Member State laws of the seized courts.

Thirdly, it remains rather vague if Chinese service providers and providers of goods, reachable via the Internet by EU customers with domicile in the EU, are under the jurisdiction of competent EU courts, even in light of EU's expansive exterritorial jurisdiction over data protection.[68] Fourthly, EU data subjects' interests are under substantial threat in reality, if Member States of their domicile have no mutual judicial assistance agreements with China to enforce EU court judgments and arbitral awards, which makes the promise to protect personal data as a fundamental right under the EU Charter of Fundamental Rights merely lip service. However, lastly, one has to pay close attention to the infamous law enforcement situation in China that is not exclusive to Chinese court verdicts only.[69] Those who intend to initiate litigation in China, or to get EU verdicts and arbitral awards enforced, have to bear

67 A significant, most recent step made last year concerns the mutual recognition of the authorized 'economic operator program' between EU and China in the context of increasing customs cooperation. arts 5 and 6 include much detailed clauses governing the treatment and protection of personal data for exchange <http://eeas.europa.eu/delegations/china/documents/news/201405161_1_aeo_mr_16_may_2014_en.pdf>.

68 Bernhard Maier, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet?' (2010) 18 IJLIT 142, 161. This is rather a country-dependent issue.

69 Zhang's discussion of the underlying problems of law enforcement in China not particularly related to foreign judgment is still sound today, since most of the circumstances he pointed out remain in reality still, some even getting worse. See Zhang (n 61) 90–95.

this in mind, when their foreign identity may tip for better enforcement, or for worse. In view of the above considerations, how the EU law can effectively protect citizens' rights to personal data and privacy in China cannot be without doubt, while the EU legislative authority has been pondering on the new General Data Protection Regulation that will be directly applied to Member States with an expansive territorial scope (Article 3 (2)) targeting data controllers not established in the Union. Under the new law, if Article 3 is to be given a broad interpretation, few if any Europeans will be taking action in China, since they will simply turn to their local Data Protection Authorities (DPAs).[70] But when the involved Chinese controllers have no establishment within the EU, how the decisions made by their local DPAs could be implemented in China remains unknown or is likely not be the case if judging from the status quo on the Chinese side.

In this case, substantial, effective efforts must be made to fulfil such the exterritorial protection promise to EU citizens to retain the authority of the future law, be it a similar Safe Harbour programme with China at the EU level, or more mutual judicial assistance agreements between Member States and China. Although the Safe Harbour Programme has been invalidated recently, this does not necessarily mean that its framework and underlying rationales are not useful and valuable in the near future as a feasible solution. But judging from China's legal development and human rights record, this is a rather difficult option, since China's privacy protection and the related legal development may not meet the rather high EU standard even in the near future, when the USA cannot even pass the judicial assessment. At this point, bilateral agreements on mutual judicial assistance seem to be a more practical choice as more supported by mutually beneficial relationships between national states. Finally, an important alternative would be more practical and desirable for EU citizens, if possible, to opt for better contractual privacy clauses, and for legislators and policy makers to promote standard contractual clauses to improve data privacy protection.

ACKNOWLEDGEMENTS

The authors would like to thank Prof Wangzhong He (China Foreign Affairs University), Weidi Long and Xingyu Yan (both from Faculty of Law, the University of Groningen) for their commenting on the first draft and Prof Dan Svantesson for his valuable, concrete advices on the latest draft. We also appreciate our anonymous peer reviewer and journal editor who helped with improving the article in many ways. Lastly, it is impossible for this article to take shape without the support of the EU EP7 Project MAPPING (Managing the Alternatives of Privacy, Property and Internet Governance).

70 This point is raised by Prof Dan Svantesson in his email communications.