27 YEARS
1987-2014

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Whys and wherefores – illegal provision under Chinese law

ChinaWhys' US/British founders sent to prison for illegally obtaining personal data. Industries that provide services to the public are at risk. By **Scott Livingston** and **Graham Greenleaf**.

In August 2014, Briton, Peter Humphrey, and his wife, naturalised American citizen, Yu Yingzeng, were convicted by a Chinese court for violating the PRC Criminal Law's prohibition on illegally obtaining the personal information of others. The couples' imprisonment provides a warning to companies operating in China on the dangers of falling foul of the country's increasingly comprehensive personal information and data privacy laws. At the same time, the Humphrey case also points to the ongoing risk of political interference in legal processes in China, further underscoring the need for companies to develop internal policies and practices in full compliance with national laws.

In this article, we look at how the PRC Criminal Law's personal information protection provision, Article 253(a), has been interpreted since its introduction in 2009. We begin with a brief account of the history of the Humphrey case, followed by an examination of Article 253(a) and its subsequent interpretation in the Humphrey and other cases.

The Humphrey Case

The Humphreys ran a Shanghai-based investigation and advisory firm,

Continued on p.3

Issue 131 **October 2014**

INTERNATIONAL report

ISSUE NO 131 OCTOBER 2014

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com
EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com
ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au
SUB EDITOR
Tom Cooper
REPORT SUBSCRIPTIONS
Glenn Daif-Burns
glenn.daif-burns@privacylaws.com
CONTRIBUTORS
Scott Livingston
Covington & Burling LLP, China
Hannah McCausland
Information Commissioner's Office, UK
Gianluigi Marino
DLA Piper, Italy
Marie Georges
Planète informatique et libertés, France
Nathan M. Crystal and Francesca Giannoni-Crystal
Crystal & Giannoni-Crystal, LLC, US
Naoya Bessho
Yahoo! Japan
Andrew A. Adams
Meiji University, Japan
Kiyoshi Murata
Meiji University, Japan
Jill Matthews
PL&B Correspondent
Merrill Dresner
PL&B Correspondent

PUBLISHED BY
Privacy Laws & Business, 2nd Floor, Monument House, 215 Marsh Road, Pinner, Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

New EU Commissioner for DP starts work in November

Vera Jourová is just one of the three European Commissioners with data protection responsibility but she is the one who will be dealing with the current negotiations on a day-to-day basis. As Jourová is not experienced in data protection, she needs to grasp the issues quickly as she wishes to complete the talks on the Regulation within six months (p.15). In terms of Safe Harbor, the EU is still waiting for answers (p.26).

The DPAs have been increasingly active in organising themselves into various groups according to issues and geographical location. The DPAs of Commonwealth countries recently met in Mauritius (p.11), where the international DPAs held their annual conference. Discussion on the EU One Stop Shop, now more realistically called the Lead Data Protection Authority, shows that there are still unresolved issues but as long as the DPAs trust each other, the concept could work well in practice (p.6). The Mauritius conference also issued a resolution on international enforcement cooperation, which will enhance the DPAs' ability to investigate data breaches that impact individuals across borders (p.8). Of course, all this will save resources as duplication of work is diminished.

On the subject of resources, there is good news from Belgium and Ireland. In Belgium, the first ever Privacy Minister has been appointed, and in Ireland the government is expected to increase the budget of the new Data Protection Commissioner, and has decided to open a new office in Dublin in addition to the current office in Portarlington. The office was originally in Dublin but was moved out of the capital in 2007 as part of a government plan to reduce the concentration of government offices there.

As always, we are grateful to our many correspondents, in this issue ranging from a Japanese Internet company to the UK Information Commissioner's Office, and writing about a variety of topical issues: the African Convention on data privacy (p.18), the Right to be Forgotten in Japan (p.27), cloud computing – comparing US and EU approaches (p.22), cookie rules in Italy (p.16), criminal law enforcement of privacy in China (p.1), and the Asian privacy scholars' conference (p.29).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Reconciling US and EU approaches to cloud contracts

Can firms, with offices in both the EU and the US, adopt a unified approach to cloud? **Nathan M. Crystal** and **Francesca Giannoni-Crystal** provide tips for choosing a provider.

Multinational organisations adopting cloud computing face different privacy issues in the US and in the EU because the approach to privacy dramatically diverges in these jurisdictions. Our paper, "Something's got to give" – Cloud Computing as Applied to Lawyers – Comparative Approach US and EU and Practical Proposals to Overcome Differences,[1] sketches the major differences between the two approaches and highlights some critical points to consider.

The two approaches originate perhaps from philosophical or historical reasons. While Europe has a general data protection law (currently based on Directive 95/46/EC but soon governed by the proposed new EU DP Regulation), which comprehensively regulates the collection, processing, transfer, and deletion of data, the US does not.

All the 28 EU members are bound by the European Commission's finding of "adequacy".[2] The Safe Harbor framework also applies to cloud providers located in the US. [3] The EU Article 29 Working Party has clarified that the Data Protection Directive "applies in every case where personal data are being processed as a result of the use of cloud computing services." (Opinion 05/2012)

While adherence to American privacy law when using cloud services basically means compliance with data breach laws (except in certain industries, see e.g. healthcare industry), compliance with EU privacy law is a major commitment when using the cloud that requires careful analysis.

Two definitions from the Directive are relevant for the cloud: "data controller" and "data processor". While a law firm using the cloud is clearly a data controller (and therefore it is fully liable for any breach of privacy law committed by the provider), the role of the cloud provider is in many cases uncertain. In a private cloud, the provider is only a data processor, while in a public cloud – where it has a greater control over data and autonomy in the choice of purpose and means of processing – the provider can also be a controller. For this reason social network providers may well be considered to be controllers under EU law. These conclusions find support in two opinions by the Article 29 Data Protection Working Party. In Opinion 1/2010, the Working Party opined on the interaction between "controller" and "processor". In Opinion 5/2012 specifically on Cloud Computing, the Working Party applied those concepts to the cloud: "[t]he cloud client determines the ultimate purpose of the processing and decides on the outsourcing of this processing and the delegation of all or part of the processing activities to an external organisation. The cloud client therefore acts as a data controller." The Working Party also opines that the general principle is that cloud providers are processors: "When the cloud provider supplies the means and the platform, acting on behalf of the cloud client, the cloud provider is considered as a data processor."

The interplay between user of the cloud and cloud provider (often providers since the cloud is increasingly a composite service) raises very complex issues of responsibilities and choice of law. In certain cases, the cloud provider is a joint controller or a controller of a different processing, so that an additional consent from law firm's clients is required. In addition, a law firm, if not otherwise subject to EU privacy law, might become subject because of the location of the provider. Article 4 of Directive makes an organisation subject to EU privacy when (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member state; . . . [OR] (c) the controller . . . for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of [the EU]..."[4] When applying these principles to cloud computing, a significant issue arises: where is a cloud "located"? Opinion 8/2010 Article 29 Working Party suggests that the location of the data is not of fundamental importance because "[i]t is sufficient that the controller carries out processing in the context of an establishment within the EU, or that relevant means is located on EU territory to trigger the application of EU law." The issue remains unclear for those controllers (for example, an American-based law firm with no office in Europe) that are not located in Europe (not having a European establishment and not using any equipment there) but that do use a cloud that might use equipment (e.g. servers) located in Europe. To complicate the issue, it is often unknown to the cloud users where cloud servers are located and where in particular their data are stored.

All these points – which are discussed in our paper - should be part of the due diligence described below.

WHAT SHOULD ORGANISATIONS CONSIDER

The following framework for analysis of cloud services has been developed for law firms but is largely applicable to any organisation.

1. Identify the type or types of cloud services that the firm is considering using and conduct a cost/benefit analysis: Three cloud service models currently exist: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS). Also, the deployment models are four: Private cloud, Community cloud, Public cloud, and Hybrid cloud. We focus on SaaS (most often in public cloud), which is the service most adopted by lawyers but the suggestions below are also useful for law firms using different service or deployment models.

For each SaaS that a firm is considering, a cost/benefit analysis

should be done to determine whether the adoption makes economic sense. In our opinion the analysis is clarified if the economic costs and benefits are evaluated before moving to a second step of evaluating the ethical and legal risks; if a service does not make economic sense, evaluation and management of risk becomes unnecessary.

A number of components of the cost/benefit analysis can be quantified, but some will be subject to a more judgmental determination. Email is probably the most ubiquitous cloud service used by lawyers. Why? While it may be unclear whether many SaaS pass a cost/benefit test, email passes with flying colors. The cost of email is minimal and may even be nonexistent, while the benefits in terms of efficiency, speed, and cost reduction through saving of postage, paper, and staff time are great. Another benefit of the cloud is that it allows lawyers to stay abreast of technology, as required by their ethical duty of competence and now expressly provided by Comment [8] to American Bar Association (ABA) Model Rule of Professional Conduct 1.15. The cloud usually allows lawyers to use the latest technologies, the software updates are automatic, and so are the backups.

2. Identify the risks associated with the particular cloud service: Lawyers have various ethical obligations that are associated with the use of cloud services and should identify the risks that could result in ethical violations, legal liability, damage to the reputation of the firm, or all of these. Especially important are the following obligations flowing from ABA Model Rule:

- Competency: Communication to a client of material information, which would include the duty to inform a client of a security breach regarding the client's data.
- Confidentiality regarding client information requiring the lawyer to use reasonable care to protect against the unauthorised disclosure of client information.
- Maintenance, preservation, and delivery of client property on termination.
- Supervision of the work of both lawyers and non-lawyers, including cloud service providers.

Violation of these ethical duties could result in malpractice or discipline for violation of duties to clients or both. Also, improper handling of data can damage the reputation of a firm, resulting in the loss of substantial business. In addition to ethical risks, there are other risks associated with the cloud: legal risks (e.g. breach of contract), security of data risks (i.e. violation of data breach laws), and "technical" risks, both external and internal risks.

Major external risks associated with SaaS are:

- Unauthorised disclosure resulting from security breaches of the provider;
- Other unauthorised disclosures resulting from inadequate procedures by providers to deal with demands for information, such as subpoenas;
- Lack of clarity about data ownership and a provider's ability to license use of data;
- Temporary loss of access to data due to Internet connection failure, provider's maintenance, or provider's failure;
- Permanent loss of data resulting from a provider's business failure;
- Geographical risks associated with location of servers housing the data in other countries where the governing law may be different;
- Problems of return of the data on termination of service.

Risks can be evaluated generally, but specific situations may create specialised risks.[6]

As for the "internal risks", they result from the firm's failure to adopt and implement policies and procedures designed to eliminate or minimise the external risks. Law firms face their own internal risks in handling data regardless of whether they use cloud services. Therefore they need to establish appropriate policies and procedures to eliminate or minimise risks associated with their own use of data (e.g., policies regarding the types of devices that lawyers can use in dealing with client data and disposal of those devices).

3. Take steps to eliminate or minimise the risk: Organisations should ask detailed questions and use reasonable care to evaluate the risks associated with use of cloud providers:

1. What is the general reputation of the provider for quality and security? Has the provider been recommended by bar associations or otherwise received recommendations or certifications from reputable businesses or organisations?
2. What are the measures that the provider takes to protect the security of the data from unauthorised access?
3. What are the industry standard measures of security?
4. Is the provider compliant with such standard measures?
5. What does the service agreement say with regard to steps the provider will take if there is a security breach to mitigate the breach?
6. What does the service agreement state with regard to notification of a security breach?
7. Does the firm have in place internal policies and procedures that require any lawyer or non-lawyer employee who learns about a security breach to notify a firm's management?
8. What does the service agreement provide with regard to notification to the firm if the provider receives a subpoena or other request for information?
9. What does the service agreement provide with regard to ownership of the data, use of the data by the provider, and licensing of the data by the provider? The agreement must provide that the law firm or the client, as the case may be, is the owner of the data. Use of subcontractors by cloud provider should only be allowed with the express written consent of the law firm or client, depending on who is the owner. In case the service agreement has a non-negotiable clause that allows the outsourcing of data, the law firm must obtain client consent to use that provider. If the service agreement allows the provider to use the data, the nature of the use must be evaluated to determine if it complies with lawyer's professional obligations and with the protection of attorney-client privilege; such use will require client consent as well, unless it is for the benefit of the client-lawyer relationship (e.g., uploading of a lawyer's time with automatic generation of an invoice).
10. What does the service agreement

provide with regard to interruption of service due to a provider's maintenance?
11. What does the service agreement provide with regard to access and recovery of data if the provider suffers an interruption of service either temporary or permanent?
12. What methods of backup of data does the provider have?
13. Does the firm have in place methods of backup and retrieval of data if the data cannot be obtained from the provider?
14. Where are the servers of the provider located? If the servers are located in other countries where the applicable law governing data security differs from that of the country of the law firm, does that foreign law apply to the data in question? If so, what steps, if any, can the firm and the provider take to avoid the storage of data in those countries (if not desirable or not allowed by law)? The location of the servers is particularly important for the application of European privacy law. Appropriate provisions could be included in the service agreement to address this issue. In case the law firm knows that the cloud servers are located abroad, prudence suggests that law firm should inform the client of this fact and obtain client consent (a law firm can do this by inserting a technology policy clause inside its retainer agreement).
15. What does the service agreement provide about return of data on termination of service?
16. Has the firm adopted appropriate policies and procedures, including training of lawyers and non-lawyers regarding use of cloud services and use of devices associated with those services?

These questions can be summarised into a shorter due diligence standard that combines the external and internal risks: in deciding whether to use a cloud service a firm should do due diligence on the provider, review the service agreement for compliance with the lawyer's professional obligations (competency, confidentiality, communication, protection of property, and supervision of non-lawyer providers) and with privacy, and institute internal policies and procedures with regard to the use of the service to comply with the firm's professional obligations.

4. Make a decision: The firm must decide whether to employ the service based on its cost/benefit analysis, identification of the relevant risks, and steps that it can take to minimise the identifiable risks. The decision is in part objective – the direct economic costs and benefits associated with the service. However, a significant part of the decision will be subjective based on anticipated benefits that are difficult to measure, e.g., projected increase in productivity, likelihood of occurrence of a risk factor, and the consequence to the firm and its clients if one of the identifiable risks materialises.

5. Post decision obligations: The cloud computing inquiry should not be static. As technology and the relevant law evolve, a lawyer's understanding should keep pace. A lawyer should:

a) periodically review current data security measures, both those of providers and internally;
b) stay abreast of best practices in data security and implement them; and
c) keep informed of changes in the law, particularly as they relate to privileges and waivers.

AUTHORS

Nathan M. Crystal, Esq, is Professor Emeritus of Professional Responsibility and Contract Law, University of South Carolina (admitted GA, NY and SC). Francesca Giannoni-Crystal, Esq., (admitted DC, NY, Italy, and in SC as FLC, not a member of SC Bar). They are both Partners at Crystal & Giannoni-Crystal, LLC (offices in New York, Washington, DC, Charleston, SC - www.cgcfirm.com
Email: info@cgcfirm.com

REFERENCES

1 *Opinio Juris* in *Comparatione* Vol. I, n.1 2014, available at www.opiniojuris-incomparatione.org/
2 On June 18, 2014, the Irish High Court referred to the EU Court of Justice a number of questions concerning the application of the Safe Harbor, the key issue being whether national judges are "absolutely bound" by a company's declaration to participate in the Safe Harbor, or whether they could still conduct their own investigations to determine if personal data are protected according to EU standards. Case 2013 765, JR, *Schrems vs. Data Protection Commissioner*. Discussion available at http://www.technethics.com/are-european-judges-still-absolutely-bound-by-the-safe-harbor/
3 Article 29 Working Group (Opinion 05/2012) and the US Department of Commerce's International Trade Administration (ITA) (Clarifications Regarding the US-EU Safe Harbor Framework and Cloud Computing) have expressed contrasting views regarding the application of Safe Harbor to the cloud industry. For the first, "sole self-certification with Safe Harbor may not be deemed sufficient in the absence of robust enforcement of data protection principles in the cloud environment", while for the latter "[s]afe Harbor continues to offer eligible US organisations, regardless of whether or not they are operating in the cloud environment, an officially recognised means of complying with the Directive's "adequacy" requirement."
4 On May 13, 2014 the ECJ held that EU privacy applies to search engines that have a branch or subsidiary in the EU that promotes the sale of the search engine's advertising space independently from where the organisation's servers are located. Decision C131/12 (known as the "right to be forgotten" decision). The Proposed Regulation sets a wider territorial scope, which will greatly impact American organisations (including law firms and cloud providers). Under the proposed new EU DP Regulation the EU privacy covers the processing of personal data by (i) a natural or legal person controlling or processing personal data established in the European Union (respectively the "controller" or the "processor"), and (ii) a controller not established in the Union, if the processing activities are related to: (a) the offering of services to data subjects in the EU; or (b) the monitoring of their behavior. Article 3.
5 www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html
6 For example, if a governmental entity (or a company dealing with the government) handles information with national security implications, special precautions and protections are required. Similarly, HIPAA requires special precautions.

Your Subscription **includes**

1. Six Reports a year
The *Privacy Laws & Business (PL&B) International* Report, published since 1987, provides you with a comprehensive information service on data protection and privacy issues. We bring you the latest privacy news from more than 100 countries – new laws, bills, amendments, codes and how they work in practice.

2. Online search function
Subscribers can search the *PL&B* website to access: back issues since 1998; special reports, slides, videos and recordings from *PL&B* events.

3. Regular e-news
Subscribers receive updates about relevant news as and when it happens. Choose international and/or United Kingdom data protection news.

4. Helpline Enquiry Service
Subscribers can request information about the current status of legislation and other information.

5. Index
Search a country, subject and company index (1987-2014) www.privacylaws.com/Publications/report_index/

Electronic Option
The electronic PDF format enables you to: receive the Report on publication; click-through from email and web addresses; and follow links from the contents page to articles.

Subscription Discounts
Discounts for 2-4 users or 5-25 users and 2 years (10%) or 3 years (15%). See www.privacylaws.com/subscribe

Privacy Laws & Business has clients in more than 50 countries, including 25 of the Global Top 50, 24 of Europe's Top 50, 25 of the UK's Top 50 in the Financial Times *lists.*

Privacy Laws & Business also publishes the United Kingdom Report, *a publication which ranges beyond the Data Protection Act to include the Freedom of Information Act and related aspects of other laws.*

Subscription Form

Subscription Packages

(VAT will be added to PDF subscriptions within the UK)

Single User Access

❑ *PL&B International* Report Subscription **£500**

❑ *UK/International* Reports Combined Subscription **£800**

Subscription Discounts

Discounts for 2-4 users or 5-25 users

Number of years: 2 (10% discount) or 3 (15%)

Go to www.privacylaws.com/subscribe

Special academic rate – 50% discount on above prices – contact the *PL&B* office

Subscription Includes:

Six new issues of each report, on-line access to back issues, special reports, and event documentation.

Data Protection Notice: *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you *do not* wish to contacted by: ❑ Post ❑ email ❑ Telephone

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel:

Email:

Signature:

Date:

Payment Options

Accounts Address (if different):

Postcode:

VAT Number:

❑ Purchase Order

❑ Cheque payable to: *Privacy Laws & Business*

❑ Bank transfer direct to our account:
Privacy Laws & Business, Barclays Bank PLC,
355 Station Road, Harrow, Middlesex, HA1 2AN, UK.
Bank sort code: 20-37-16 Account No.: 20240664
IBAN: GB92 BARC 2037 1620 2406 64 SWIFTBIC: BARCGB22
Please send a copy of the transfer order with this form.

❑ American Express ❑ MasterCard ❑ Visa

Card Name:

Credit Card Number:

Expiry Date:

Signature: Date:

Please return completed form to:
Subscriptions Dept, Privacy Laws & Business,
2nd Floor, Monument House, 215 Marsh Road,
Pinner, Middlesex HA5 5NE, UK
Tel +44 20 8868 9200 Fax: +44 20 8868 5215
e-mail: sales@privacylaws.com 24/10

www.privacylaws.com

Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.