大江橋法律事務所|翰凌律师事务所

中国法律速递

OH-EBASHI | HANLING

CHINA LEGAL NEWSLETTER

July 2022

Articles

For inquiries, questions or comments, please contact us at info_china@ohebashi.com or suny@hanlinglaw.com

【Oh-Ebashi LPC & Partners Website】https://www.ohebashi.com/en/

【Hanling & Partners Website】http://www.hanlinglaw.com/en

大江橋法律事務所|翰凌律师事务所
中国法律速递
OH-EBASHI | HANLING
CHINA LEGAL NEWSLETTER

Legal Compliance of Workplace Surveillance in China -From a Personal Information Protection Perspective

Hanling & Partners
Yuchuan Sun
PROFILE

A few months ago, a piece of rather interesting news in China raised debates about to what extent an employer can impose surveillance upon its employees in workplaces. The news reported that one major e-commerce company in China has internally announced sanctions upon some of its employees on the ground of excessive access to work-irrelevant mobile applications during work hours. The company was able to collect various data such like the length of access or quantity of data that has been exchanged by each particular employee's use of his or her mobile phones to access certain applications (Tik Tok or online shopping applications) via the company's internal wireless network. Those who support such an action argues that workplace surveillance is necessary to maintain the employment disciplines as well as the security. While others think such a surveillance scheme is only an undue intrusion to employees' privacy.

No matter what stance to take, it is a fact that workplace surveillance has been an ordinary practice since long before. It is fair to say that employers have genuine needs to apply surveillance to ensure a safe and efficient workplace. Sometimes such surveillances are even mandatory by relevant laws. But as a matter of nature, surveillance upon employees is, more or less, a form of intrusion to employees' privacy.

In China, the problem of workplace surveillance has long been addressed and discussed mainly as an employment law matter. Although there are not many relevant cases, the courts usually treat workplace surveillance as a part of the employer's internal management and admit the legality of surveillance measures so long as the employer has included such a surveillance scheme in the internal regulation and such regulation has been adopted and circulated to the employees through proper procedures.

However, with the adoption and enactment of the Personal Information Protection Law (the "PIPL") in the year of 2021, a new important dimension has been added when we consider this problem. Workplace surveillance has become more than a mere employment management issue.

I. Personal Information or Not?

Before we answer the question whether the information collected via workplace surveillance constitutes personal information under the PIPL, we shall first look at what kind of information are usually being collected and processed by employer via workplace surveillance.

- ***Communication Information.*** Perhaps the workplace surveillance is most frequently applied to scenarios of all types of communication occurred in the workplace. Usually, information gathered from surveillance upon communication can be further categorized into "Traffic Information/Meta information" or "Contents Information". Traffic information usually means information that generated from communication activities themselves. Such like the dial-in/dial-out number, length of access, length of conversation, e-mail address, website or IP address visited or quantity of data. While the "Contents Information", as the word explains itself, means the contents that have been communicated through such communications.
- ***Biometric Information.*** Biometric information is another important category of information that may be generated and processed by workplace

surveillance, especially when an employer uses facial recognition, fingerprint recognition or CCTV system for security or other purposes.

- ***Other Information.*** Such like real-time location information of particular employee.

Now, we shall turn to the question as whether the fore mentioned information will fall into the scope of "personal information" under the PIPL. The "personal information" is defined by the PIPL as any "information in relation to an identified or identifiable natural person that is recorded electronically or otherwise". Like the concept of "personal data" under GDPR, "identified or identifiable natural person" and "in relation to" are the two most important building blocks of the concept of the "personal information". However, in a workplace context, since employees are almost always "identified" to the employers, the part of "in relation to" will play a more important role here.

The word of "in relation to" itself is rather easy to understand, but the question as to what extent shall a piece of information be regarded as "in relation to" to a particular natural person is actually quite a difficult question and matters greatly in practice. Will a piece of information be regarded as personal information even if such an information only has a very remote or indirect relation to the particular natural person? Should information about an object or property owned by a natural person be deemed as "in relation to" such natural person? The essential question here is "what level of relevance does it require to render a piece of information to be personal information"?

The PIPL has not provided any further explanation about the question. But according to WP29's "Opinion 4/2007 on the concept of personal data", a piece of information will constitute "personal data" under GDPR if such information is "about a natural person" (the "content" element), or "for a natural person" (the "purpose" element) or "may have an impact upon a natural person" (the "result" element). The Content Element means a piece of information will be regarded as related to a natural person if such information is *about* a particular natural person while all surrounding circumstances shall be assessed. The Purpose Element means when a piece of information is used or likely to be used to *evaluate or treat* a natural person, then such information shall be treated as related to such natural person. Finally, the Result Element means when, after an assessment of all surrounding circumstances, a piece of information is *likely to cause an impact* on a natural person, it may be considered as "related" to such a natural person.

Based on the approach under GDPR, it is clear that information collected and processed by employer through workplace surveillance is very likely to fall into the scope of personal information. Because, first of all, the purpose of workplace surveillance is to monitor and evaluate behaviors of employees thus renders the "purpose element" exists in most cases. And, workplace surveillances are usually accompanied by measurements and consequences that may cause impact on employees, like the news that has been introduced at the beginning of this article, which will establish the "result element". Still no need to mention that quite a part of the data collected through workplace surveillance are directly related to the employees. Therefore, employers shall be aware of the fact that workplace surveillances are not mere an employment law matter but may also be regulated by the PIPL.

II. How to Secure the Lawfulness Ground?

If implementation of workplace surveillance falls into the processing of personal information, then the next key question will be how to ensure a lawfulness ground for such processing.

According to the PIPL, in principle, processing of personal information will only be lawful if the data subject provides consent to such processing. However, consent will not be required where the processing of personal information is necessary for the conclusion or performance of a contract to which the relevant natural person is a party or is necessary to carry out human resource management, or where processing of personal information is necessary for the performance of statutory duties or obligations, or where processing of personal information is necessary to respond to public health emergency, to protect life, health and property safety of natural person in an emergency, or where processing of person information for the purpose of new report and public opinion supervision, or process disclosed personal information within a reasonable scope. And in the scenario of workplace surveillance, employers are very likely to rely on "consent" or "human resource management" to secure the lawfulness ground.

Because, unlike the GDPR, the PIPL does not exempt consent by date subject while there are "legitimate interests"

for a processor to process personal information. Thus, obtaining consent from employees looks the most approachable lawfulness ground to be relied on. When rely on "consent", according to the PIPL, the processor shall ensure that such consent is "explicitly and freely given". But it is very debatable if a consent provided by an employee to its employer in an employment context will constitute a true consent. In GDPR, a consent must be "freely given", "specific" and "informed" to be a true "consent". And the word "freely given" usually means that the data subject had "genuine choice" at the time of consent and had the right to refuse or withdraw such consent. If an employee provides his or her consent only from a fear of any unfavorable treatment by the employer that may follow if he or she refuses to provide such consent, then such consent can hardly be regarded as a "explicitly and freely given".

When rely on "human resource management", the employers shall also keep in mind that not all workplace surveillances are necessary to carry out human resource management. For example, if an employer installed surveillance cameras to ensure the safety of the workplace, or monitor the employee's use of network for the purpose of maintaining cybersecurity or to record employees' movements upon certain files or documents to protect the trade secrets, it is questionable whether such surveillances can be regarded as a necessary measure to carry out human resource management.

III. Minimization

After a lawful ground has been secured for workplace surveillance, employer shall further consider if the surveillance measurement has met the minimization principle. Article 6 of the PIPL says processing of personal information shall with clear and reasonable purpose and shall be directly related to such purpose, collect personal information in such a manner that will cause minimum effect to the natural person's rights and interest within the minimum scope that is necessary to achieve the purpose of processing with any excessive collection of personal information.

In order to meet such minimization principle, employer shall keep the processing of personal information within reasonable scope by using measurements that are proportionate to the purpose of processing. The employer shall not carry out the surveillance in a relatively "intrusive" manner when there is only a relatively less important purpose to achieve or such purpose can still be achieved with a less intrusive manner.

For example, in the case of the news that has been mentioned at the beginning of this article, if an employer wants to avoid employees spending too much time on irrelevant mobile applications or websites, the employer can simply ban or restrict access to certain mobile applications or websites instead of monitoring employees' activities of using the network. Banning access to certain mobile applications or websites can achieve the purpose with almost same effects without any necessary to process employees' personal data or any intrusion to employees' privacy.

Therefore, it is advisory for the employer to, before the implementation of workplace surveillance, carefully review its surveillance scheme to make sure that such surveillance cannot be substituted with other less intrusive method and such surveillance has been minimized in terms of scope, quantity, duration and storage.

IV. What to Inform?

No matter whether a consent by the data subject is required or exempted to process personal information, according to the PIPL, the processor shall always keep the date subject informed of the processing. Article 17 of the PIPL is clear about what shall be informed to the data subject before any processing starts. According to this article, a processor shall at least inform the data subject of the purpose of processing, method of processing, types of personal information to be processed and the duration of storage.

To ensure that employees are well informed of the surveillance measures is not only necessary to meet the transparency requirement. As mentioned above, while employers are most likely to obtain employees' consent to build the lawfulness ground, under the context of employment whether a consent by an employee to the employer constitutes a valid consent under the PIPL remains questionable. Therefore, a proper and adequate notice or statement to employees regarding the surveillance measures before the employees render their consents may be a practical way to increase the likelihood that such consent will be deemed as a valid one.

Generally speaking, it is advisory for the employers to keep employees informed of the following information before

they render their consents to be subject to the surveillance measures.

- ***Rules and regulations of using employer's network, computers and other devices.*** Those rules and regulations usually include the time, method and scope on using the employer's network, computers and other devices. It must be clear about whether the employer's devices can be used for private purposes and if there is any restriction on such use for private purposes.
- ***Purposes and measures of the surveillance.*** The employer shall inform the employees of all the surveillance measures that are being applied or will be applied and purpose of each surveillance measure respectively. Also the employer shall keep the employees informed of the key facts about all surveillance measures including subject of surveillance, scope, technical method, duration and frequency. The employer shall make an individual statement to draw the employees' attention if any sensitive personal information may be collected and processed as a part of any surveillance measure.
- ***Possible Consequences that may arise from the surveillance.*** The employees shall be aware of the consequences, in advance, when any inappropriate behaviors were detected through surveillance measures and if there is any remedy that the employee could rely on.
- ***Security measures.*** The employer shall also make an explanation to the employees about all the security measures both from organizational perspective and technical perspective that have been implemented to safeguard the information collected through surveillance measures.
- ***Others.*** Such as the name of the processor if any surveillance measure is wholly or partly outsourced to a third party, possibility of transfer of personal data collected through surveillance measures to an overseas entity.

V. In the End

With the advancement of technology, surveillance measures with higher efficiency and less cost will continue to be added to the tool box, thus be more widely applied in the real life. But employers shall be aware of the fact that the adoption of the PIPL in China has added a new dimension to the regulation scheme of workplace surveillance. It will no longer be a mere employment law issue.

In the context of personal information protection, lawfulness requirement is the first question that any processor shall take into careful consideration. Although remain questionable, since the PIPL does not admit "legitimate interest" as one lawfulness ground, employers in China are likely to rely more on employees' consent to meet the lawfulness requirement. Thus, it will be advisory for the employers to make a careful and prudent consideration before implementation of any workplace surveillance to avoid or at least reduce the legal compliance risk.

For inquiries, questions or comments, please contact us at info_china@ohebashi.com or suny@hanlinglaw.com

大江橋法律事務所|翰凌律师事务所
中国法律速递
OH-EBASHI | HANLING
CHINA LEGAL NEWSLETTER

China's Life Sciences and Healthcare-No.2
—The Good Vigilance Practice rule in China

Oh-Ebashi LPC & Partners
Fumi Takatsuki
PROFILE

Hanling & Partners
Yuchuan Sun
PROFILE

I. China GVP

This article will introduce the drug vigilance activities required by the new Good Vigilance Practice ("GVP"), enacted on May 7, 2021, and come into effect on December 1, 2021. The GVP will be applied to MAHs and NDA applicants conducting clinical trials.

Before the adoption of the GVP, the Administration Measures on Reporting and Monitoring of Drug Failure Reactions (Ministry of Health Order No. 81, effective as of July 1, 2011) and the Public Notice of the State Pharmaceutical Administration on Report of Adverse Drug Reactions (the "No. 66 Notice") issued in 2018 constituted the basic legal framework of monitoring and reporting of adverse drug reactions in China. According to the NMPA's explanation, NMPA will amend the Administration Measures on Reporting and Monitoring of Drug Failure Reactions (Ministry of Health Order No. 81) and apply it to the drug vigilance activities conducted by medical institutions and drug sales companies (wholesale and retail).

II. Applicable Entity

The GVP applies to MAHs (domestic and overseas) and the applicants for new drug registration authorized to conduct clinical trials. Existing MAHs must register the prescribed information in the National Drug Failure Response Observation System (http://www.adrs.org.cn/) within 60 days of the effective date of the GVP.

III. The Internal Pharmaceutical Vigilance Department

According to the GVP, the MAH must establish a drug safety committee and a department dedicated to drug alert operations ("PV Department") within the company, which must have clear job responsibilities and a good cooperative relationship with other departments. Usually, the drug safety committee shall be consisted of the legal representative or major management personnel, the drug vigilance officer ("PV Officer"), the head of the quality control department, and the managers of the related departments. The duties of such committee are to handle critical PV matters such as reviewing and deciding on significant risks, handling major or urgent events and determining risk control policies (Articles 19 and 20 of the GVP).

The MAH's legal representative or major management personnel shall, in general, be responsible for PV activities. They shall designate the person(s) responsible for PV, assign sufficient numbers and personnel of commensurate qualifications, provide the necessary resources, and reasonably organize, coordinate, and ensure the effective operation of the PV system and the realization of quality objectives.

Regarding the requirements for personnel related to PV operations, the PV Officer must (a) hold a managerial position, (b) have a professional background in medicine, pharmacy, epidemiology, or a related specialty, (c) have a university degree or higher or a professional technical qualification of intermediate level or higher, (d) have experience in PV related work at least three years and (e) be familiar with the laws, regulations, and technical guidance principles related to drug PV operations in China, as well as knowledge and skills related to PV management operations.

In addition, MAHs should register the PV Officer in the

National Drug Defective Reaction Observation System (If there is a change in the registered information, it must be re-registered within 30 days).

Other personnel in the PV department are not required to have certain years of experience but there must be sufficient staff placed in the department. They must have professional background in medicine, pharmacy, epidemiology, or a related specialty, received PV related training, be familiar with the principles and possess the knowledge and skills which are necessary to handle PV operations (Articles 23, 24, and 26 of the GVP).

Furthermore, MAHs are allowed to outsource PV-related work to domestic companies with the expertise, management systems and resources, and are allowed to outsource work to other MAHs in the same group. But MAHs must sign an outsourcing contract, monitor and inspect the performance of the contractor on a regular basis.

IV. Internal Audits

MAH shall conduct internal audits ("Internal Audits") regularly to audit the PV systems and company-internal rules and their enforcement and evaluate the PV system's adequacy, sufficiency, and effectiveness. MAHs shall promptly conduct an internal audit whenever there is a significant change in the PV system. MAHs may conduct the internal audit independently, systematically, and comprehensively by designating personnel or outside personnel or experts.

Records of internal audits shall be duly produced and reserved. A written report shall be prepared, including the audit's essential circumstances, contents, and results. For problems discovered by the internal audit, MAHs shall investigate the cause, take appropriate corrective and preventive measures, and track and evaluate the corrective and preventive measures.

V. Monitoring and Reporting Adverse Drug Reactions

(1) Information collection channels, evaluation, and methods

MAHs must establish channels for collecting information on adverse drug reactions from medical institutions, drug sales companies, patients, other individuals, etc. MAHs must ensure that relevant persons may easily reach to MAH via telephone numbers or e-mails published on the instructions, drug packages, website, etc. And MAHs can collect information through academic literature research, post-marketing safety studies, etc.

MAH shall evaluate the reports based on the following items.

(i) Transmitting the original records: whether the documents' truthfulness, completeness, and traceability have been maintained in transferring the original forms.

(ii) Follow-up: follow-up on missing information regarding reporting severe or unanticipated adverse reactions.

(iii) Assessment of predictability: MAHs must evaluate the predictability of adverse drug reactions. An adverse reaction shall be deemed as unpredictable if the characteristics, severity, or outcome of the negative response is not inconsistent with the drug attachments description.

(iv) Assessment of severity: an adverse reaction shall be deemed as severe if any of the following occurs: death, life-threatening, requiring hospitalization or prolonged hospitalization, permanent or significant disability/function, those with congenital anomalies or congenital disabilities, other medically substantial events.

(v) Assessment of relevance: assessment of the relevance relationship between the suspect drug and the reaction that occurred in the patient in accordance with the criteria for assessing the relevance classification class of drug adverse reactions published by the National Drug Failure Reaction Monitoring Center.

(2) Reporting of adverse reaction

Report of adverse reaction shall contain adverse reactions related to quality problems of the drug, prescribing over indications, over dosages and contraindications.

MAHs should submit a report to the regulatory authority about severe adverse reactions within 15 days at the latest and non-serious adverse reactions within 30 days. In the case of a severe adverse reaction to a drug used outside of the country, the MAHs must submit a report to the regulatory authority about each adverse reaction. If the MAHs need to suspend the sale or use of the product or remove the product from the market outside of the country due to a defective reaction, MAHs must submit a report within 24 hours.

(3) Identification and evaluation of safety risks (detection and evaluation of signals)

The GVP newly defines the concept of signal detection and requires that signals must be detected by appropriate methods, such as review and inspection of individual drug

adverse reaction report, case series evaluation, human detection methods such as case report summary and analysis, and computer-assisted detection methods such as data mining. It also stipulates the frequency of detection of signals, the types of signals to be focused on, the factors to be considered when decide the priority, the principles of signal evaluation, and the procedures to be taken when clustered signals are detected (however, as the content of GVP about the evaluation of signals is only a set of principles, detailed regulations are expected to be issued later).

(4) Post-marketing safety studies of pharmaceutical products

The GVP requires that post-marketing safety research on pharmaceutical products should be conducted in compliance with GCP (if applicable), and the post-marketing safety research (which is needed by NMPA), the research plan, and the result report must be submitted as required by the regulatory authority.

(5) Risk communication and PV plan

The GVP states that MAHs must communicate drug safety information to healthcare professionals, patients, and the public and conduct risk communication for drugs, such as publishing documents for healthcare professionals and drug guides for patients and holding presentations.

The PV plan must include an overview of drug safety, drug alert activities, and a description of planned risk management measures, timing, a cycle of implementation, etc. The PV Officer must review and confirm the plan and report to the MAH's drug safety committee for review and confirmation.

(6) Documents, records, and data management

MAHs must establish a well-developed system for vigilance management. Regarding the management of relevant documents, records, and data, MAHs shall establish rules about a retention period (at least ten years from the expiration of the drug registration certificate for drug alert data and records) and procedures for their management and maintain a master file, which shall be updated from time to time to reflect current conditions. The drug alert master file shall include at least the following.

(i) Organizational structure: describes the organizational structure, responsibilities, and interrelationships as they relate to PV activities.
(ii) Basic information on the PV Officer: including an area of residence, contact information, biography, responsibilities, etc.
(iii) Deployment status of full-time staff: including the number of full-time staff, their professional backgrounds, responsibilities, etc.
(iv) Sources of information on suspected adverse drug reactions: the main channels and methods of collecting data on suspected adverse drug reactions.
(v) Information tools or systems: the information about tools or systems used in the PV activities.
(vi) Management system and regulations: An overview explanation of the PV management system, an inventory of PV management systems and rules.
(vii) Operational status of the PV management system: describes the situation of monitoring and reporting of adverse drug reactions, identification, evaluation, and control of drug risks, etc.
(viii) Outsourcing of drug alert activities: Provide a list of outsourcing contracts, details of outsourcing, deadlines, contractors, etc.
(ix) Quality control: Explain the quality control situation of PV. Include quality objectives, quality assurance system, quality control indicators, internal audits, etc.
(x) Appendix: Include system and operating rule documents, drug list, contractor agreement, internal audit report, revision history of the master file, etc.

For inquiries, questions or comments, please contact us at info_china@ohebashi.com or suny@hanlinglaw.com

OH-EBASHI LPC & PARTNERS

Ryo Matsumoto
Partner, Shanghai Office and Osaka Office
Chief Legal Representative of Shanghai Office
PROFILE

Ko Matsui
Partner, Tokyo Office
PROFILE

Fumi Takatsuki
Partner, Osaka Office
PROFILE

Masafumi Takeda
Counsel, Tokyo Office and Shanghai Office
PROFILE

HANLING & PARTNERS

Qun Ji
Representative Partner
PROFILE

Yuchuan Sun
Partner
PROFILE

Hongbin Weng
Partner
PROFILE

Ting Zhang
Associate
PROFILE

Pengcheng Zhang
Associate
PROFILE

For inquiries, questions or comments, please contact us at info_china@ohebashi.com