AMNESTY INTERNATIONAL 國際特赦組織香港分會

Telecommunication Companies

Personal Information Collection, Use and Disclosure

Best Practice Guidelines

1. Information collection process

1.1. When and how to collect information:

1.1.1. Consent should be obtained upon or prior to collecting service subscribers' personal information.

1.1.2. Consent must be freely given, specific, informed and unambiguous.

1.1.3. Use explicit consent provisions whenever possible.

1.1.4. Consider the sensitivity of the personal information involved when determining the appropriate type of consent (express or implied). As a general rule, more sensitive data (e.g., medical or financial information) should have explicit consent.

1.2. When collecting personal information, the data user should inform service subscribers in a Personal Information Collection Statement that is written in unambiguous language comprehensible by a diverse audience. The Statement should include, but not limited to the following elements:

1.2.1. The legal basis of personal information collection and disclosure.

1.2.2. What personal information is being collected.

1.2.2.1. Service providers must identify for service subscribers what personal information is being, or may be, collected about them.

1.2.2.2. Service subscribers cannot be required to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service – they must be given a choice. These choices must be explained clearly and made easily accessible.

1.2.3. With which parties personal information is being shared

1.2.3.1. Information disclosures to third parties must be clearly explained, including the types of information being shared and the purpose of the disclosure.

1.2.4. The purposes of personal information collection and disclosure.

1.2.4.1. Service subscribers should be made aware of all purposes for which information is collected, used or disclosed.

1.2.4.2. Service subscribers should be informed of their rights to access, review, amend, withdraw their personal information.

1.2.4.3. Service subscribers should be informed of the identity and specific authorities of the data user.

1.2.4.4. Provide service subscribers with adequate information to access the service providers privacy policies and practices.

1.2.4.5. Service subscribers must be informed of the risks and consequences

2. Limits to Information Collection

2.1. Service provider should not collect, use, and disclose information that is beyond what is necessary to provide the product or service, or required by law.

2.2. Service provider must seek explicit consent from individual when collecting information other than those as prescribed in 2.1. Service subscribers should be given the opportunity to choose whether to disclose such information.

2.3. Service providers must seek explicit consent from service subscribers in case of significant changes such as using personal information for a new purpose that was not originally consented upon.

2.4. Genetic and biometric data shall not be collected at all times.

2.5. Identifiable GPS and other geographical location information shall not be collected, used and disclosed unless individual has given explicit consent and the information collected should be used and disclosed for emergency purpose only.

2.6. Service providers must classify categories of sensitive data (such as identifiable financial, health, biometric, genetic, political opinions, religious beliefs, sexual orientation etc.) and specific what enhanced security measures are being applied to protect sensitive data.

3. Information Disclosure

3.1. If service subscribers have given consent to disclose their information to third parties, the following information must be made available to them:

3.1.1. Details of third parties: disclosures to third parties must be clearly explained and the information of third parties should be specified as specific as possible, including the identity of third parties, their type of businesses and the service they provide.

3.1.2. Types of information shared: service subscribers should be informed of the types of information being shared with corresponding third parties.

3.1.3. Service providers should inform service subscribers what types of information will be disclosed in aggregated or anonymised manners, whereas which types will not.

3.1.4. Purpose of information disclosure: service providers should provide information in specifying the purpose of information disclosure. These purposes must be described as specific as possible in unambiguous language, avoiding ambiguity terms such as “internal research” or “service improvement” (for instance, if the mailing of monthly statement is outsourced to a third-party subcontractor, service subscribers should be informed of the details of the subcontractor, and as to what types of personal information that the subcontractor is handling).

3.1.5. In the case where third parties may change periodically, such information should be updated and made known to the affected service subscribers in a timely and easily accessible fashion.

3.1.6. Service providers should inform service subscribers under what circumstances and legal requirements that personal information will be disclosed to third parties or law enforcement agencies without their prior knowledge and consent, such information should be made known to service subscribers in an easily accessible fashion.

3.1.7. Ensure all third parties involved have adequate security measures in place for information transfer and storage.

4. Information process and storage

4.1. All personal information shall be protected from loss or theft, and from unauthorized access, use, alteration, copying, disclosure, and destruction.

4.2. Establish security safeguards appropriate and proportional to the sensitivity of the personal information, and the nature of the possible risks.

4.3. All personal information collected is not to be transferred to countries without adequate data protection legislation.

4.4. All personal information collected should be retained no longer than is necessary for the purposes for which the personal information are processed, preferably no longer than one year after the termination of service subscription.

4.5. Designate specific personnel the authorization to access, process and control personal information, while restricting employee access (including information technology staff) to personal information for unrelated and non-business reasons. Include appropriate disciplinary measures for violation.

4.6. Provide adequate and regular privacy training for staff and specific personnel.

4.7. Service providers should state clearly in their privacy policies and practices in unambiguous language that is easily accessible by a diverse audience and must include, but not limited to, the following personal information protection information:

4.7.1. Specify the security measures in place to protect the storage and transfer of non-sensitive and sensitive personal information (for instance specific hardware and software, firewall, pseudonymization, anonymization, encryption, masking etc.)

4.7.2. Specify the location where personal information will be stored

4.7.3. Specify the time period of personal information will be retained

4.7.4. Specify the personnel with authorities to access, process, and control personal information

5. Personal Rights

5.1. Detailed of person rights should be made known to service subscribers in unambiguous languages that is easily accessible to them.

5.2. Personal rights of service subscribers should include the followings:

5.2.1. Right to Information

5.2.1.1. Establish a free, simple, clear and accessible mechanism for service subscribers to inquire and review:

5.2.1.1.1. What types of personal information have been collected and stored.

5.2.1.1.2. The purpose of information collection, process and disclosure.

5.2.1.1.3. To what third parties the information has been disclosed.

5.2.1.1.4. How their personal information is being protected, processed and transferred.

5.2.1.1.5. Information (name, position, location, and contact information) of designated personnel with authorities to access, process and control personal information should be made known to service subscribers in an easily accessible fashion.

5.2.2. Right to access and rectification:

5.2.2.1. Establish a free, simple, clear and accessible mechanism for individuals to:

5.2.2.1.1. Access their personal information upon request.

5.2.2.1.2. Rectify their personal information when necessary.

5.2.2.1.3. Correct or destroy personal information found to be incorrect, incomplete, irrelevant, or inappropriate, as quickly as possible

5.2.2.1.4. Right to withdrawal

5.2.2.1.5. Right to object to data processing

5.2.2.2. Establish a free, simple, clear and accessible mechanism for individuals to:

5.2.2.2.1. Withdraw their personal information.

5.2.2.2.2. Withdraw their consent.

5.2.2.2.3. Withdraw the use and disclosure of personal information to third parties.

5.2.2.2.4. Withdraw the collection, use and disclosure of personal information for specific purpose that does not distress the continue supply of necessary service.

5.2.2.2.5. Service providers should delete all related person information (both private and public) upon withdrawal of personal information and consent.

5.2.2.2.6. Should there is circumstance that various personal information may need to be retained after the service subscribers have withdrawn (for instance email addresses in “do not contact” list or due to other legal requirements), service providers must inform service subscribers what information will be retained and for how long.

6. Monitoring mechanism

6.1. Establish procedures to receive and respond to complaints and questions about all aspects of compliance with your posted privacy policy and practices in a free and easily accessible fashion.

6.2. Establish a complaint and dispute resolution process that is effective, fair, impartial, confidential, understandable, easy to use, and timely.

6.3. Inform service subscribers of third-party complaint, investigative and dispute resolution procedures available to them.

6.4. Inform service subscribers of their legal rights and obligations.

6.5. Inform service subscribers of governmental complaint and judicial remedy mechanisms available to them

6.6. Establish an action plan that will be taken in case of information breach (for instance reporting time, investigation procedures/personnel/task force etc.)

6.7. Conduct and publish internal and transparent digital security audits on an annual, if not quarterly basis.

6.8. Conduct and publish transparent digital security audits on third parties and subcontractors on an annual, if not quarterly basis.

6.9. Publish a Government Assistance Report that disclose the volume of law enforcement agencies' legitimate demands on interception of the content of customer's communications and disclosure of customers' communications related data ('metadata') on an annual basis.