Australian Library and Information Association

ALIA library privacy guidelines for ebook lending and digital content provision

ALIA Constitution Objects addressed:

- To promote the free flow of information and ideas in the interest of all Australians and a thriving culture, economy, environment and democracy; and
- To promote and improve the services provided by all kinds of library and information agencies.

ALIA Core Values addressed:

- Connection of people to ideas, knowledge creation and learning
- Dedication to fostering reading, information and digital literacies
- Adherence to information privacy principles
- Excellence, accountability, integrity and responsibility in service to our communities
- Partnerships and collaborations to advance these values.

Principle

This guideline is intended to provide library and information professionals with guidance on negotiating third party digital licensing or agreements and the appropriate management and security practices in respect to library customers' personal information.

The rapid advancement of technology has resulted in increasing privacy implications for libraries. Libraries enter into licences or agreements with commercial information content providers in order to provide library customers with access to digital information, including e-books, journals, and databases.

Customer privacy in libraries has become widely challenged as vendors engaged by library services may collect data on users' activities, communications, and transactions as a condition of providing their content or services.

The optimum licence agreement would require library customers to provide only a valid library card to access digital content services, without the need to provide any personally identifiable information. These licensing agreements are rare, as more and more companies collect

personally identifiable information from library customers accessing the content and setting up personal accounts within the library's subscription.

When libraries are negotiating third party digital licences or agreements the following principles should be addressed.

Guidelines

Notice and disclosure - *What information will be collected and how it will be used.*

Customers should be given notice of the industry partner's information practices and policy before any personal information is collected from them. This includes how the data will be used, potential recipients of the data, whether the requested information is voluntary or required. The data should only be used for the purpose stated and not for any other purposes. Customers should also have the ability to view the data collected, and also verify and contest its accuracy.

Consent - *Personal choice and control*

Industry partners will not disclose personal information without the customer's consent. Customers should also be provided with options to control how their data is used. Typically this is an 'opt-in' or 'opt-out' model where customers affirmatively give permission for their information to be used for other purposes. In addition, customers are given options to tailor the information to fit their preferences by checking boxes to grant or deny permission for specific purposes rather than using a simple "all or nothing" method.

Accessible and understandable privacy policy

To be effective the industry partner's privacy/collection policies should be clear and conspicuous, in a prominent location, and readily accessible from both the site's home page and any web page where information is collected from the customer. The wording should be easy to follow, providing customers with meaningful and effective notice of what will happen to the personal information they are asked to disclose.

Robust network and data integrity and security

This includes the steps taken by the company to ensure the confidentiality, integrity and quality of the data and the means by which it is collected. Security involves both managerial and technical measures to protect against loss and the unauthorised access, destruction, use, or disclosure of the data. Managerial measures include internal organisational approaches that limit access to data and ensure that those individuals with access do not utilise the data for unauthorised purposes. Technical security measures to prevent unauthorised access include encryption in the transmission and storage of data. Industry partner sites must be HTTPS.

Privacy policies meet the current standards and Australian legislation

Industry partners must meet the core principles of data privacy protection. There must be mechanisms to ensure that customers have a simple and effective way to have their concerns addressed and the ability to hold companies accountable for not following privacy policies, standards or legislation. There must be mechanism in place for the reporting to individuals and authorities where there have been data breaches as per the *Privacy Amendment (Notifiable Data Breaches) Bill 2016*.

Collaboration

Libraries and industry partners must work together to ensure that the contracts and licences governing the provision and use of digital content meet libraries' policies, and legal obligations regarding user privacy.

In instances where the library is unable to negotiate robust privacy protections, customers should be clearly advised when they are no longer being protected by the library's privacy policy. Libraries should encourage users to be aware of the implications and provide guidance in data protection and privacy protection.

Links

- The Privacy Act 1988 (Privacy Act) https://www.legislation.gov.au/Series/C2004A03712
- Australian Privacy Principles. https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles
- Universal Declaration of Human Rights (UN General Assembly,1948).
- IFLA Principles for Library eLending https://www.ifla.org/elending/principles

Adopted 2018.