Privacy Commissioners Issue Joint Guidance On Bring Your Own Device Programs

An organization's information can be put at risk when staff begin to bring their own devices and use them in the workplace. As a result, in such cases, an organization should consider adopting an appropriate "bring your own device" (BYOD) program to seek to manage the risks inherent in such activity.

Generally, a BYOD program allows an organization's employees to use their personal mobile devices for both personal and business purposes. A threshold issue for an organization is to consider what devices may be included in a BYOD policy, as society has moved far past smart phones to all sorts of wearable devices that can capture, process and post an organization's confidential information and the personal information of its staff and customers. While there are many benefits to a BYOD program (*e.g.*, an increase in employee satisfaction and productivity), organizations should evaluate the various inherent risks associated with the implementation and use of a BYOD program, and take reasonable steps to mitigate such risks.

To support this process, the Office of the Privacy Commissioner of Canada, along with its provincial counterparts in Alberta and British Columbia, recently released a new joint guidance document (*Is a Bring Your Own Device (BYOD) Program the Right Choice for Your Organization?)* which highlights various key privacy and security risks that should be considered when making decisions regarding a BYOD program. The following is a brief summary of a few of these considerations:

- **Conduct a Privacy Impact Assessment (PIA) and Threat Risk Assessment (TRA)**: Conducting a PIA and TRA will help identify and address risks associated with the collection, use, disclosure, storage and retention of personal information. These assessments may lead an organization to restrict the use of applications with, for example, cloud services.
- **Develop, Communicate, Implement and Enforce a BYOD-Specific Policy**: Establishing the obligations and expectations of BYOD users is essential to the prevention of privacy and security threats. Organizations are encouraged to work with internal departments, such as information technology, information management, legal, finance and human resources, to develop an enforceable, easy-to-understand BYOD policy. Such a policy should address issues such as user responsibilities, acceptable and unacceptable uses of BYOD devices, application management and access requests.
- **Mitigate Risks Through Containerization**: *Containerization* refers to the compartmentalization of an organization's corporate information from any other

information that may be resident on an employee’s mobile device. Undertaking this process creates a clear division as to what is subject to an organization’s BYOD policy and what is not.
- **Formalize a BYOD Incident Management Process**: Despite any effort to address all privacy and security risks, organizations should be cognizant that vulnerabilities will continue to exist. In the event of a privacy or security breach, organizations should accordingly have an incident management process in place to help with the identification, containment, reporting, investigation and correction of that breach in a timely manner.
- **Maintain an Inventory**: In order to minimize privacy and security threats, organizations should maintain an up-to-date inventory of authorized mobile devices and apps participating in its respective BYOD program. Maintaining such an inventory will help an organization to, among other things, take appropriate steps during an incident response.

Employees whose personal mobile devices are improperly secured put all of the information on the mobile device, include the organization’s confidential information, at risk. Thus, an organization may suffer significant harm, including financial loss, loss of competitive advantage and/or damage to its reputation, if any such device is lost, stolen, jailbroken or rooted.

This does not mean that an organization should avoid a BYOD program. Increasingly staff are demanding such programs, so it may become a recruiting and retention issue. However, the organization should seek to create a secure environment where the benefits of a BYOD program can be enjoyed, and where the risks are minimized, by: (i) setting up suitable and appropriate BYOD policies; (ii) educating users on those policies; (iii) supervising user conduct under the policies; and (iv) implementing suitable technological measures to support those policies.

If your organization needs assistance with its BYOD program, please feel free to contact a member of Bennett Jones’ privacy team.