Office of the Privacy Commissioner of Canada

Office of the Information and Privacy Commissioner of Alberta

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

News Release

Privacy guardians urge caution for businesses contemplating a Bring Your Own Device Program

Federal, British Columbia and Alberta privacy commissioners issue guidelines to help organizations reduce risks for personal information when considering allowing employees to use their own mobile devices and computers for work

August 13, 2015 — With the line between work and home increasingly blurred, bring your own device (BYOD) programs are growing in popularity and raising significant concerns among privacy guardians about the protection of personal information.

In an effort to assist organizations that are considering introducing a BYOD program, the Office of the Privacy Commissioner of Canada and the Alberta and British Columbia Information and Privacy Commissioners' Offices have issued joint guidelines aimed at mitigating risks of security incidents and privacy breaches.

"Allowing employees to use their mobile phones, tablets and laptop computers for both personal and professional use carries significant privacy risks – particularly when one world collides with the other," says Privacy Commissioner of Canada Daniel Therrien. "Companies need to consider the risks in advance and prepare to manage them effectively. Only then could they conclude whether a BYOD program is right for them."

According to the guidelines, organizations should conduct a privacy and threat assessment prior to implementing a BYOD program to identify and address risks associated with the collection, use, disclosure, storage and retention of personal information.

Rules governing the acceptable use of devices, corporate monitoring, the sharing of devices, app management, connection to corporate servers and responsibility for security features, software updates and voice or data plans should also be explicitly laid out in a BYOD policy.

"Both IT professionals and staff participating in BYOD programs need to be trained on acceptable use policies and other responsibilities. Without buy-in from senior management, companies may not provide the resources and support needed to effectively implement these programs to protect both employers and employees," adds Jill Clayton, Information and Privacy Commissioner of Alberta.

Other suggested risk mitigation measures include encrypting BYOD devices, authentication and partitioning devices to keep approved corporate apps and data separate from personal apps and data.

"Companies also need to bear in mind that despite their best efforts, bad things can happen. Devices may be lost or stolen and personal information may be compromised," says Elizabeth Denham, Information and Privacy Commissioner for British Columbia.

"Having a formal incident management response plan in place is crucial to ensuring incidents are detected, contained, reported, investigated and corrected in a consistent and timely manner – as is employee training and awareness of the privacy and security risks."

- 30 -

See also:

Is a Bring Your Own Device (BYOD) Program the Right Choice for Your Organization? *Privacy and Security Risks of a BYOD Program*

Contemplating a Bring Your Own Device program? Consider these tips

For more information, please contact:

Office of the Privacy Commissioner of Canada
Tobi Cohen
E-mail: tobi.cohen@priv.gc.ca
Telephone: 819-994-5619

Office of the Information and Privacy Commissioner of Alberta
Scott Sibbald
SSibbald@oipc.ab.ca
780-422-9048 / 1-888-878-4044

Office of the Information and Privacy Commissioner for British Columbia
Cara McGregor
cmcgregor@oipc.bc.ca
250-217-5535