BYOD – It Can Be Privacy And Security Protective

On December 11, 2013, Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian, and TELUS released a new whitepaper applying the principles of Privacy by Design to employee owned devices in the workplace. The whitepaper, entitled "Bring Your Own Device: Is Your Organization Ready?", sets out a five-step process for developing and implementing a BYOD program. Those steps are:

- **Step One: Establishing Requirements – End-User Segmentation**. This involves identifying user needs.
- **Step Two: Technology Alignment and Device Choice**. This involves aligning permitted devices to user needs and operational considerations, as well as the level of access permitted based on the device characteristics.
- **Step Three: Policy Development**. In this step, the organization is to develop policies and procedures governing information security, monitoring, privacy, guidance on the use of wifi, termination of employment and other issues engaged by BYOD.
- **Step Four: Security**. This step requires the organization to evaluate existing and implement additional administrative, technical and physical security controls to enhance or maintain the security of the organization's IT infrastructure and the integrity and privacy of personal information.
- **Step Five: Support**. In this final step, an organization to have a plan to support employees, including with respect to lost or misplaced devices.

There is one place where I might part company with the Information and Privacy Commissioner's Whitepaper. In my view, a BYOD policy is insufficient to address the complexities of managing security and privacy expectations and the cooperation required by employees and information technology and security professionals.

Last month, I had the pleasure of speaking on a panel with JoAnn Sochor, AVP Social Media Compliance at TD Financial Group, and Nyree Embiricos, counsel at Amex Bank of Canada regarding social media and BYOD in financial institutions.

In our presentation, I strongly recommended an annual User Participation Agreement that sets clearly the rights and responsibilities of the user and the employer.

Article by Timothy Banks

About Dentons

Dentons is a global firm driven to provide you with the competitive edge in an increasingly complex and interconnected marketplace. We were formed by the March 2013 combination of international law firm Salans LLP, Canadian law firm Fraser Milner Casgrain LLP (FMC) and international law firm SNR Denton.

Dentons is built on the solid foundations of three highly regarded law firms. Each built its outstanding reputation and valued clientele by responding to the local, regional and national needs of a broad spectrum of clients of all sizes – individuals; entrepreneurs; small businesses and start-ups; local, regional and national governments and government agencies; and mid-sized and larger private and public corporations, including international and global entities.

Now clients benefit from more than 2,500 lawyers and professionals in 79 locations in 52 countries across Africa, Asia Pacific, Canada, Central Asia, Europe, the Middle East, Russia and the CIS, the UK and the US who are committed to challenging the status quo to offer creative, actionable business and legal solutions.

Learn more at **www.dentons.com**

For more information, visit our Data Governance Law blog at **www.datagovernancelaw.com**