



**FOR IMMEDIATE RELEASE**

June 20, 2007

**MINISTRY OF SMALL BUSINESS AND REVENUE FAILED TO ADEQUATELY PROTECT PERSONAL INFORMATION, COMMISSIONER FINDS**

**Victoria**—In a report issued today, Information and Privacy Commissioner David Loukidelis found that improper browsing of a database by an employee of EDS Advanced Solutions Inc., a Ministry of Small Business and Revenue service provider, was a violation of s. 30 of the *Freedom of Information and Protection of Privacy Act* (“FIPPA”). Section 30 requires public bodies to make reasonable security arrangements to protect personal information from risks such as unauthorized access, collection, use, disclosure or disposal.

The complainant, a woman, learned that her ex-husband had claimed he could get her home address through a friend of his at the Ministry, whose identity the complainant knew. The complainant feared for her safety and complained to the Ministry. Investigation revealed that the Ministry employee had not accessed the complainant’s information on the database, but that an employee of EDS, a Ministry service provider, had done so. Further investigation revealed that the EDS employee had been engaged in inappropriate browsing of personal information in the database for at least 3 months.

The Commissioner concluded that, while the breach was caused by unauthorized improper behaviour of the EDS employee, it had gone undetected because of insufficient technical security measures, including a lack of real-time audit capacity. The Commissioner also found that, by taking more than nine months to notify affected individuals that their personal information had been inappropriately accessed, the Ministry and EDS had breached their s. 30 obligations.

Following the breach, the Ministry and EDS have taken significant steps to improve security and to develop employee awareness of, and compliance with, privacy law. Expressing his satisfaction at the steps since taken by the Ministry and EDS, the Commissioner said, “This case proves that privacy breaches can result from individual snooping, but it also shows that government has to take information security seriously up-front. It’s not good enough to wait for a breach before you act. The law requires more.” The Commissioner also added that, “When a privacy breach is discovered, you have to act quickly to stop it and to consider how to help those affected. You need to act fast, especially if there are safety risks or identity theft risks.”

-30-

For further information contact:  
Mary Carlson, Executive Director  
Office of the Information and Privacy Commissioner  
Phone: (250) 387-5629  
Cell: (250) 415-5533