McINNES COOPER
BARRISTERS SOLICITORS & TRADE MARK AGENTS
focus on PRIVACY LAW

Spring 2003

Beware Default Settings:

Privacy Commissioner Findings Affect All Website Operators

David T.S. Fraser - david.fraser@mcinnescooper.com

Since Canada's new privacy law came into force, the Office of the Privacy Commissioner has released two findings that demand close attention from any company that operates a website. Businesses without websites are definitely in the minority, so this means almost all companies are affected.

CANADA'S NEW PRIVACY LAW

The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") is Canada's new private sector privacy legislation. It came into force on January 1, 2001 for the federally-regulated private sector and will be binding upon the provincially regulated private sector on January 1, 2004.[1] It places strict limits on how organizations can collect, use, disclose and retain personal information. The fundamental tenet of PIPEDA is that informed consent must be obtained before collecting, using and disclosing personal information.

THE LEGAL ENVIRONMENT

Even though PIPEDA applies only to federally-regulated companies until January 1, 2004, the Office of the Privacy Commissioner has been called upon to address complaints related to website functions, most of which are transparent to the users.

In Finding #25,[2] the Complainant had noticed that upon visiting a broadcaster's website his computer's firewall indicated that the broadcaster's server had attempted to connect to his computer. (In most cases, visiting a website involves a two-way connection, but is only initiated by the visiting computer. This connection is via a designated networking protocol using a

[1] A quick test of whether a company is federally or provincially regulated is to ask whether the company is subject to the *Canada Human Rights Act* and the *Canada Labour Code.* If the answer is yes, the company is most-likely federally regulated for the purposes of PIPEDA .

[2] Available online at: http://www.privcom.gc.ca/cf-dc/cf-dc_011120_e.asp

specific port on the computer.) In this case, the broadcaster's advertising server attempted to connect using a Microsoft Windows service known as NetBios[3]

The Commissioner found that NetBios information, in this circumstance, was "personal information" under PIPEDA. From the published "finding":

> The Commissioner was satisfied that in some circumstances, notably the complainant's, a NETBIOS might be used to obtain information traceable to an identifiable individual. He determined therefore that the information at issue was personal information for purposes of the Act.

Principle 4.3 listed in Schedule I of PIPEDA requires the consent of the individual for the collection, use and disclosure of personal information. The Commissioner concluded that seeking a website visitor's NetBios name, even unintentionally, was a violation of PIPEDA: it was collecting personal information without consent.

The broadcaster's webmaster was not aware that automatic NetBios connections were enabled by default when he upgraded his system. Upon being notified of this, this function was disabled and the Commissioner concluded the complaint was "well-founded and resolved."

Most recently, the Office of the Privacy Commissioner received a complaint about a website operated by an airline. As set out in the Commissioner's finding #162,[4] the complainant alleged that the airline had violated Principle 4.3 – Consent, which is in Schedule I of PIPEDA. Specifically, the airline's website placed "cookies" on the hard-drives of visitors and would not permit access by individuals who had disabled cookies on their systems.

Cookies are small snippets of text code that are placed on a user's computer by a website's server. Usually they are inserted without the knowledge of the user, often from sites that users are not aware they have visited.[5] Cookies allow for a greater personalization of a user's experience on the internet, as was presumably the purpose of the airline about whom the complaint was made in this particular finding. The cookies on the airline site "remembered" the user's language preference and whether they wanted the Canadian or US-focussed version of the website.

The airline's website placed cookies on the hard-drives of visitors but did not disclose this practice in the "terms of use" document for the website. By doing so, the Privacy Commissioner found that the airline had contravened the requirement from Principle 4.3 that informed consent be obtained before collecting personal information.

The other count of this complaint dealt with an alleged refusal of service to visitors who set their web browsers to refuse cookies. Principle 4.3.3 says that:

---

[3] NetBios is a default Windows networking service that, among other things, allows computers in a local workgroup to be named. NetBios is not necessary for internet communications and most security commentators suggest the service be disabled.

[4] Available online at http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030416_7_e.asp.

[5] For more information on cookies, visit the "Unofficial Cookies FAQ" at http://www.cookiecentral.com/faq/.

> An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

In short, a company cannot refuse service simply because the customer did not consent to the collection of personal information that is not necessary for providing that service.

The airline's website would not allow access beyond the "splash page" unless a user's browser was set to accept cookies. The airline said this was a glitch it promptly fixed upon having it brought to their attention. Even if this denial of access was unintentional, the Privacy Commissioner determined the airline contravened principle 4.3.3.

WHAT THESE FINDINGS MEAN FOR COMPANIES

Any company that operates a website needs to carefully consider how the website server software collects personal information from its users. Though some may not consider this to be "personal information", as commonly understood, the privacy legislation contains an expansive definition of the term:

> "personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

Particulars about an individual's computer and any use of "cookies" appear to constitute personal information.

Companies need to be additionally aware of how default settings on some computer software collects personal information in a manner that may present undue risk under PIPEDA.

Existing websites should be carefully examined as part of a company's due diligence and compliance efforts in preparation for the deadline of January 1, 2004. Companies in the federally-regulated private sector, such as the broadcaster and the airline referred to in the Commissioner's findings, are already subject to PIPEDA and should include websites within their ongoing compliance efforts.

THE MCINNES COOPER METHOD

The McInnes Cooper Privacy Working Group has devised a standardized protocol to help our clients determine areas where current practices may not be in compliance with PIPEDA. We will identify vulnerabilities and rank them in order of risk. We can then address any problem areas in order of priority.

Our standardized protocol involves three phases:

(i) preliminary screening,
(ii) comprehensive risk assessment, and
(iii) implementation.

The protocol can be applied enterprise-wide or to a particular business line. The members of the McInnes Cooper PIPEDA team are skilled in providing training for key managers and employees, raising awareness of PIPEDA and providing instruction on compliance. Clients with internal training programs can take advantage of our abilities to "train the trainer." We have resources such as model policies and checklists to save clients the time and expense of building systems from the ground up. As a continuing source of value, our clients will have access to regular updates as this new area of regulation evolves.

If you have any questions related to PIPEDA or provincial privacy law, please contact any of the following:

Nova Scotia
David T.S. Fraser
902 424 1347
david.fraser@mcinnescooper.com

New Brunswick
Jaime Connolly
506 458 1544
jaime.connolly@mcinnescooper.com

Newfoundland
Jackie Penney
709 724 8239
jackie.penney@mcinnescooper.com

Prince Edward Island
Paul Kiley
902 629 6268
paul.kiley@mcinnescooper.com