



CANADIAN PRIVACY LAW REVIEW

Volume 8 • Number 2

January 2011

In This Issue:

Privacy Class Actions Are Here, But Do We Need Them?

Wendy Matheson, Patrick Flaherty and Krista Stout.....13

“Third Persons” and “Implied Consent”: The Court of Appeal Analyses Quebec’s Privacy Act in the Context of Grievance Arbitration

Lukasz Granosik.....20

PIPEDA Proposed Amendments: M&A Uncertainty Reduced

Natalie Zinman, Hugh Christie and Nicholas Dietrich.....21



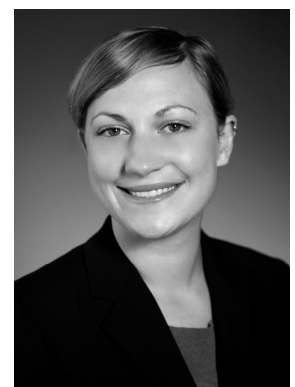
Privacy Class Actions Are Here, But Do We Need Them?



Wendy Matheson
Partner
Torys LLP



Patrick Flaherty
Partner
Torys LLP



Krista Stout
Associate
Torys LLP

While some people advocate for the infamous position taken by Sun Microsystems co-founder Scott McNealy 11 years ago — *You have zero privacy anyway; get over it!*¹ — the recent proliferation of privacy class actions suggests that reports of the “death of privacy” may be greatly exaggerated.

The amount of personal information² available to and used by businesses is increasing exponentially, as is the seeming inclination of many people to air their private lives online. At the same time, just as many people seem to be increasingly concerned with protecting their privacy, and media attention has focused on the ways in which personal information may be misused. It is not surprising that the debate about the importance of protecting personal information rages on.

These conflicting views have not stopped the inevitable trend toward bringing privacy class actions. And as we have come to expect, this trend first appeared in the United States, and has now taken hold in Canada. However, the conflicting attitudes toward privacy are evident when it comes to the question of damages. What if there are none? Why should the court system be engaged at all? These issues are coming to the forefront of a landscape that accommodates two quite different kinds of privacy claims:

Canadian Privacy Law Review

The **Canadian Privacy Law Review** is published monthly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Suite 700, Markham, Ont., L3T 7W8, and is available by subscription only.

Web site: www.lexisnexis.ca

Design and compilation © LexisNexis Canada Inc. 2010. Unless otherwise stated, copyright in individual articles rests with the contributors.

ISBN 0-433-44417-7 **ISSN 1708-5446**

ISBN 0-433-44418-5 (print & PDF)

ISBN 0-433-44650-1 (PDF)

ISSN 1708-5454 (PDF)

Subscription rates: \$205.00 plus GST (print or PDF)
\$320.00 plus GST (print & PDF)

Editor-in-Chief:

Professor Michael A. Geist

Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law
E-mail: mgeist@uottawa.ca

LexisNexis Editor:

Boris Roginsky

LexisNexis Canada Inc.
Tel.: (905) 479-2665 ext. 308
Fax: (905) 479-2826
E-mail: cplr@lexisnexis.ca

Advisory Board:

- **Ann Cavoukian**, Information and Privacy Commissioner of Ontario, Toronto
- **David Flaherty**, Privacy Consultant, Victoria
- **Elizabeth Judge**, University of Ottawa
- **Christopher Kuner**, Hunton & Williams, Brussels
- **Suzanne Morin**, Bell Canada, Ottawa
- **Bill Munson**, Information Technology Association of Canada, Toronto
- **Stephanie Perrin**, Service Canada, Integrity Risk Management and Operations, Gatineau
- **Patricia Wilson**, Osler, Hoskin & Harcourt LLP, Ottawa

Note: This Review solicits manuscripts for consideration by the Editor-in-Chief, who reserves the right to reject any manuscript or to publish it in revised form. The articles included in the *Canadian Privacy Law Review* reflect the views of the individual authors and do not necessarily reflect the views of the advisory board members. This Review is not intended to provide legal or other professional advice and readers should not act on the information contained in this Review without seeking specific independent advice on the particular matters with which they are concerned.

- claims arising from mishaps or crime
- claims challenging business practices

Although both types of claims engage privacy concerns and present liability risks for businesses, the legal and strategic issues can be very different. An inadvertent security breach will have its challenges, but does not usually cut to the heart of the business model in the way a challenge to business practices can. Illustrative U.S. cases are discussed below, as well as their Canadian counterparts. Most of these cases are recent or settled, or were otherwise disposed of without needing the determination of many of the issues that the courts will ultimately have to confront, with respect to both certification and the merits.

Class Actions Arising from Mishaps or Crime

It is increasingly common to read, in the media, about the unintended disclosure of personal information and about privacy-related crime: the documents in the dumpster, still visible to the walker-by; the disk shipped to the wrong address; the vendor who forgot to scrub the servers before resale; and the stolen laptop. Class actions have been commenced seeking relief for the inadvertent transmission of customer information to third parties;³ the improper disposal of personal information in public dumpsters or landfills;⁴ the simple mistake of leaving a document in the wrong place;⁵ the loss or theft of portable devices with databases containing personal or sensitive financial information;⁶ the interception of consumer data by hackers;⁷ and the disclosure of customers' email addresses to third parties who subsequently send spam mail.⁸

Mishaps

Mishaps involving personal information have triggered a number of class action claims. For example, in the U.S. case *Pinero v. Jackson Hewitt Tax Service Inc.*⁹ plaintiffs commenced a class action against the second largest professional tax service firm in the world for allegedly disposing of its customers' tax returns in a public dumpster. Someone fished the returns out of the dumpster and contacted local media and law enforcement, which in turn identified and notified the lead plaintiff. While Jackson Hewitt alleged that the documents were stolen, it was not clear how these documents came to be disposed of so publicly. In another U.S. example, AOL, the Internet service and media giant, was sued for alleged breaches of federal electronic privacy law after AOL temporarily and accidentally posted nearly 20 million keyword searches of approximately 658,000 AOL members on a public website. Certain keywords

contained personally identifiable information¹⁰ that, when combined, could lead to identification of the user. Although AOL removed the information, it continued to be accessible on other sites that had already reposted it. The release of the data in this case prompted widespread criticism from privacy advocates and Congress. AOL was faced with both a class action and a Federal Trade Commission complaint over the inadvertent disclosure.

In Canada, cases have also arisen from accidental disclosure of personal information. For example, some 366 staff of the Joyceville Correctional Institution sought certification of a class action against Correctional Services Canada for leaving an employee list with home contact information in an unlocked cabinet in an open, unsecured hallway in the jail.¹¹ When the list was retrieved months later, some names on the list were highlighted, and it could not be determined how many inmates had seen the list. The class action alleged that the disclosure violated the privacy and constitutional rights of the prison guards. A settlement was reached in 2010 under which class members each received \$1,000 to compensate for the breach of privacy.

Crime

Computer crime can result in major data breaches. Where personal information is involved, privacy complaints seem inevitable. *In Re Heartland Payment Systems, Inc. Data Security Breach Litigation*¹² is an excellent example. In what was described by analysts as one of the largest data breaches ever reported, Heartland Payment Systems, Inc., a U.S. payment processor, was faced with a total of 17 consumer class actions and ten bank and credit unit class actions arising from an alleged security breach involving the theft of sensitive financial information associated with credit and debit cards. In 2007, hackers breached Heartland's computer security and intercepted transaction data using malware (malicious software). The hackers, who have since been indicted, allegedly stole or exposed approximately 130 million credit and debit card numbers and corresponding personal information.

Both consumers and financial institutions made claims. The myriad of claims included allegations that Heartland failed to uncover the security breach until notified by third-party credit card companies, delayed notifying customers of the breach and did not offer affected individuals any credit monitoring services or other relief. Heartland eventually settled in 2010.

These types of claims typically allege negligence in developing and maintaining security measures to protect against data breaches; sometimes they allege breach of an express or a contractual term regarding security in the agreement between the business and the customer, among other claims. In some cases, the focus of the claim is not the mishap itself, but the delay in notifying its customers and the appropriate authorities, thus preventing them from taking steps to mitigate any harm arising from the breach.

Class Actions Arising from Business Practices

Lately, several class actions have been commenced that challenge a company's business model and handling of personal information. Online services that actively encourage users to provide, use and share personal information are finding themselves in the crosshairs. An increasing number of plaintiffs are saying that they place a premium on the safety and security of their personal information, and that they have a reasonable expectation that businesses will protect this information. They claim that a business's use or disclosure of personal information has exposed them to various harms, including identity theft, harassment and embarrassment.¹³

These allegations typically fall into one of three categories: (i) that the company acquired, used or disclosed customers' personal information without prior authorization or consent; (ii) that the company contravened its own privacy policy; or (iii) that the company diverted users' private data to third-party providers of targeted advertising for profit. Several current actions combine elements of all three.

This year, for example, a putative class action was filed in California on behalf of Facebook users challenging the site's new default privacy settings. The complaint alleged that the new settings provide users with less control over their personal information with the pre-selected (or "pre-clicked") disclosure as the default option, leading "unwary users into inadvertently revealing large amounts of information about themselves, placing their personal safety and financial security at risk."¹⁴ It was further alleged that personal information was disclosed to third parties, such as Google, which then placed targeted ads on the users' profile pages.

Similarly, a U.S. class action was filed in 2010 against Google in connection with its social networking product Google Buzz for alleged violations of federal, state and common law privacy laws.¹⁵ The program automatically suggested a "follower/following" list, based partly on whom the user emailed and chatted with most frequently online. The complaint alleged that by automatically requiring users to opt in, Google allowed users' private data to be shared with the Buzz public network without adequate notice or user consent. Google settled the action, despite having announced modifications to its privacy settings to enhance user control shortly after the launch of Google Buzz.

In Canada, class actions have been brought to challenge an element of a company's business model. In *Union de Consommateurs v. Bell Canada*,¹⁶ for example, a proposed class action was brought in Quebec against Bell Canada on behalf of Internet subscribers who complained about Bell's alleged "throttling" practices. The claim alleged that Bell deliberately slowed consumer services during peak hours, favouring business users. It further alleged that Bell violated subscribers' privacy rights by using a technology called "deep packet inspection." This technology allegedly allows Bell, without prior notice or consent, to access and collect the content of all messages sent by subscribers using Bell's Internet service.

Law Still Developing

Most of these claims are at early stages. Some have settled. There is little definitive judicial discussion about the many issues that arise regarding certification and liability. There are also significant differences between the U.S. and the Canadian legal landscapes. Many of the privacy class actions in the United States are based on statutory causes of action that are not available in Canada. Most commonly relied on are the *Electronic Communications Privacy Act*¹⁷ and the *Computer Fraud and Abuse Act*.¹⁸ Both these statutes provide a cause of action for damages for specific misuses of technology, including the improper interception, disclosure or intentional use of electronic communications; the intentional accessing of a computer without authorization; or the knowing transmission of a harmful program or code.

Another major difference arises because U.S. courts have long recognized invasions of privacy as tortious. Canadian plaintiffs do not have the same legal foundation, though a foothold is emerging, albeit not fully formed.¹⁹ And it remains to be seen whether some of the privacy legislation in Canada can found a claim for damages. These are all issues that will no doubt arise as privacy claims continue to become more common in Canada.

Notice Practices

There is no doubt that notification can give rise to litigation, whether meritorious or not. The notice of a privacy breach, giving rise to a concern about potential harm, is enough to persuade some people to sue.

Notification practices are still developing. Only some legislation requires notification.²⁰ The federal *Personal Information and Protection of Electronic Documents Act* [PIPEDA]²¹ does not require notification, but that may soon change. Under proposed amendments in Bill C-29 that are now being debated at second reading, the federal Privacy Commissioner must be notified of "material breaches." The bill provides some guidance on which factors are relevant to determining materiality,

including the sensitivity of the information, the number of individuals affected and the organization's assessment of whether the breach indicates systematic problems. Further, the bill introduces a requirement for notification to individuals where it is reasonable to believe that the breach creates a "real risk of significant harm to the individual," considering the sensitivity of the information and the probability that the information has been or will be misused. Further notification requirements are also set out in the bill.

To meet consumer expectations and to mitigate any damage, businesses may and sometimes do voluntarily decide to notify affected individuals. For example, after a security breach of its online job application database in May 2009, the insurer Aetna Inc. publicly announced the breach, sent notification letters directly to 65,000 of its current and former employees, and offered credit monitoring services and identity theft insurance.²² Similarly, in February 2008, the Bank of New York Mellon Inc. gave notice after it learned that a third party had lost back-up tapes containing the electronic banking information of customers of People's United Bank. BNY Mellon offered individuals whose information had been compromised \$25,000 in identity theft insurance, free credit freezes, and first a year — and then two years — of credit monitoring.²³

*'Of the estimated 640,994 Connecticut residents who may have been affected by the February 2008 tape loss, about 91,000 have signed up for the free Experian credit monitoring service being paid for by BNY Mellon,' Department of Banking Commissioner Howard Pitkin said. 'We know that BNY Mellon has spent \$3.48 million to provide credit protections for Connecticut residents following the data breach, and recognize that they are taking responsible action to minimize its impact to consumers.'*²⁴

Depending on the circumstances, notice may be helpful, but it may also only serve to ensure that the company is sued, even if no damage is caused by the breach.

Is There Any Real Damage?

Not every privacy breach ought to result in monetary relief. One issue that must be confronted in privacy class actions is the reality that despite a breach, there may be no damage whatsoever. A number of U.S.

lawsuits have been unsuccessful because of the class members' inability to prove "actual harm," and courts have been consistent in dismissing class action complaints on this basis.²⁵

The remedies sought in these actions vary, but often include the cost of credit monitoring, the cost of closing and opening financial accounts, any actual costs associated with identity theft or fraud, and damages for emotional distress.²⁶ The main focus, however, remains the risk of identity theft. According to a recent study, identity theft increased in the United States by 11 per cent from 2008 to 2009, affecting nearly 11 million Americans.²⁷ In Canada, it is estimated that 6.5 per cent of Canadian adults or nearly 1.7 million people have been affected in this way.²⁸ It is, however, not at all clear that all instances of alleged identity theft are well-founded.

U.S. courts have consistently held that until identity theft occurs, there is no demonstrable actual harm. The risk of identity theft is too speculative to constitute a compensable injury. Furthermore, some U.S. courts have found that the claims for the costs of protective measures, including credit monitoring, are linked not to actual harm but to the fear of some undefined potential harm, and thus are not recoverable.²⁹ The cases on this point are "nearly uniform in not allowing recovery where there is only a risk of injury and no actual misuse of the stolen electronic data."³⁰ Courts have dismissed class action complaints on this basis.

The relevance of actual harm has also been recognized in Canada. In a recent Quebec case, *LaRose c. Banque Nationale du Canada*,³¹ the Quebec Superior Court authorized a class action in connection with the theft of three laptops, one of which contained personal information of a group of mortgagees of National Bank. The Court noted that under Quebec law, the fear of identity theft or fraud does not constitute a harm or injury in and of itself and cannot provide the basis for a class action. It was only because there was some evidence of actual identity theft that certification was granted.

The range of benefits provided in privacy class action settlements also reflects the uncertainty that often surrounds a claim arising from a privacy breach.

Settlements often do include reimbursement of out-of-pocket expenses incurred after a breach. For example, in the *Heartland* settlement, an initial actual damages settlement fund of \$1 million was established for the reimbursement of reasonable out-of-pocket expenses (including phone or postage costs, third-party charges due to card cancellation or replacement, and unauthorized account charges). Certain funds permit recovery for a reasonable amount of time spent to address the breach, or for free credit monitoring or identity theft protection;³² others cap the individual recoverable amount.³³

Companies have also agreed to change a specific program or policy to dispel privacy concerns raised by class litigants. These measures may include clarifying terms of use and control over privacy settings associated with a specific program;³⁴ changing security measures, including full encryption of data;³⁵ providing an informational “privacy toolkit”;³⁶ completely redrafting a company’s privacy policy;³⁷ or undertaking to retain an independent third party to do a privacy audit of the business.³⁸

Some settlements are more focused on assuaging a general concern, without any apparent financial consequences. In one U.S. settlement, for example, class plaintiffs who brought a putative action alleging a technical violation of a statute regulating credit and debit card transactions³⁹ were awarded settlement vouchers for \$50 off certain store purchases or for a “classy” T-shirt or hoodie. Similarly, in the *TJX Companies* settlement, arising out of hackers’ unauthorized access to the company’s computer network, class plaintiffs were given vouchers for use in TJX stores, as well as a bonus of a One Day Customer Appreciation Sale. Again, in *Parker v. Time Warner*,⁴⁰ a class action was brought against the cable provider for allegedly breaching subscriber policy provisions of the *Cable Communications Policy Act of 1984*⁴¹ by collecting

and disclosing personally identifiable information without giving subscribers proper notice. As part of the settlement, class members were offered the choice of one free month of cable service, two free movies on demand or a \$5 cheque.

When no real harm has occurred, class proceedings may well be a completely unnecessary endeavour. During the course of a motion to approve the final settlement of the class action brought against Time Warner Entertainment, the Court expressed its concern that the combination of consumer protection statutes (containing statutory damages provisions) and class action mechanisms may threaten defendants with liability that is far in excess of the actual harm. Although the Court reserved its opinion on whether these actions should be certified for trial, it questioned the desirability of settlement when a minimal sum is made available for the purported victims of a minimal harm and so much time and labour is expended to achieve so little:⁴²

Over the course of more than a decade, Class Counsel has logged over 12,000 hours to achieve a final result that evokes ambivalence. The alleged wrongs of Time Warner — technical violations of the Cable Act — were essentially righted long ago when the company changed its privacy notice and discontinued its list sales business. However, the litigation continued for eight years as a quest for some measure of direct compensation for the Class Members, the vast majority of whom were all the while oblivious to the purported violations and essentially unharmed by them.⁴³

These issues should be considered at the certification stage as well, to ensure that a class proceeding is, in fact, the preferable procedure. Similarly, there are other possible arguments against the use of class actions for all types of privacy concerns, including the availability of statutory privacy complaint processes.

As the volume of cases continues to expand both north and south of the border, the courts will have to confront these issues. It remains to be seen whether privacy claims will become routine class claims when considered on their merits and when certification is thoroughly debated in contested court proceedings.

¹ Quoted by Chantal Bernier, Assistant Privacy Commissioner of Canada, “Privacy Preoccupations: The policies and practices of

the Office of the Privacy Commissioner of Canada” (Remarks to the Public Sector Executive Network in Ottawa, January 26, 2010). Online: <http://www.priv.gc.ca/speech/2010/sp-d_20100126_cb_e.cfm>.

“Personal information” is defined in the federal *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, as “information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.”

Speevak v. Canadian Imperial Bank of Commerce, [2010] O.J. No. 770, 2010 ONSC 1128.

Class Action Complaint, *Pinero v. Jackson Hewitt Tax Service Inc.*, No. 08-3535 (E.D. Louisiana 2008) [*Jackson Hewitt Tax Service*]; *Cole v. Prairie Centre Credit Union Ltd.*, [2007] S.J. No. 493, 2007 CarswellSask 519 (Q.B.).

Jackson v. Canada, [2005] O.J. No. 2691 (Ont. S.C.).

Ruiz v. Gap, Inc., 2010 WL 2170993 (C.A.9 (Cal.)); *McLoughlin v. People’s United Bank Inc. and Bank of New York Mellon, Inc.*, 2009 U.S. Dist. LEXIS 78065 (D. Conn. 2009) [*People’s United Bank and Bank of New York Mellon*]; *In Re Department of Veterans’ Affairs (VA) Data Theft Litigation*, 653 F. supp. 2d 58 (D.D.C. 2009); Notice of Settlement, Union Pacific Data Breach Class Action Settlement (D. Nebraska 2007) [Notice of Settlement, Union Pacific]; *Bell v. Acxiom Corporation*, 4:06-cv-00485-WRW (E.D. Ark. 2006) [*Acxiom Corporation*]; *Jackson v. Canada, ibid.*; *Waters v. DaimlerChrysler Financial Services Canada Inc.*, [2009] S.J. No. 382, 2009 SKQB 263; *Bordoff v. Gestion D’Actifs CIBC Inc./CIBC Asset Management Inc.*, filed in the Quebec Superior Court on January 23, 2007, [2010] Q.J. No. 10334, Court File No. 500-06-000383-071.

In re Heartland Payment Systems, Inc., No. 4:09-MD-2046 (S.D. Tex. 2010) [*Heartland*]; Class Action Complaint, *Ryan v. Delhaize America, Inc. d/b/a Sweetbay, and Hannaford Bros. Co.* (D. Maine 2008) [*Delhaize America*]; *Wong and Churchman v. The TJX Companies Inc. [TJX Companies]*, filed in the Ontario Court of Justice on January 26, 2007, [2008] O.J. No. 398, Court File No. CV-07-0272-00.

In re Ameritrade Accountholder Litigation, C-07-2852-VRW (N.D. Cal. 2009); *Cherry v. Emigrant Bank*, 604 F. Supp.2d 605 (S.D.N.Y. 2009) [*Emigrant Bank*].

Jackson Hewitt Tax Service, *supra* note 4.

“Personally Identifiable Information” has been defined by the FTC as “individually identifiable information from or about an individual [consumer] including, first and last name; home or other physical address; email address or other online contact information; telephone number; social security number; persistent identifier (i.e. customer number held in a “cookie” or processor serial number that is combined with other information that identifies an individual) ...”, as cited in *Valentine v. WideOpen West Finance LLC* (2010 U.S. Dist. LEXIS 90566) at para. 25(d).

Jackson v. Canada, *supra* note 5.

Heartland, *supra* note 7.

Class Action Complaint at 2, *Silvestri v. Facebook, Inc.*, No. C10-00429 (N.D. Cal. 2010) [Class Action Complaint, *Facebook*].

Ibid. at 3.

In Re Google Buzz User Privacy Litigation, No. 5:10-CV-00672-JW (N.D. Cal. 2010).

Filed in the Quebec Superior Court on July 8, 2008, [2009] J.Q. no 16640, Court File No. 500-06-000436-085.

18 U.S.C. § 2510-2522 (2006).

18 U.S.C. § 1030 (2006).

Somwar v. McDonald’s Restaurants of Canada Ltd., [2006] O.J. No. 64 at para. 31.

For example, the Ontario *Personal Health Information Protection Act*, S.O. 2004, c. 3, Schedule A.

Supra note 2.

Allison v. Aetna, Inc., No. 09-2560 (E.D. Penn. 2010) at 2 [*Aetna*].

People’s United Bank and Bank of New York Mellon, *supra* note 6.

Connecticut Department of Banking, “Department of Consumer and Department of Banking Announce Settlement with Bank of New York Mellon for 2008 Data Breach” (February 3, 2009).

See, for example, *Ruiz v. Gap*, *supra* note 6 (summary judgment in favour of defendant affirmed for failure to plead cognizable injury); *Aetna*, *supra* note 22 (court finds plaintiffs lack standing due to the speculative nature of the damage alleged); *People’s United Bank and Bank of New York Mellon*, *supra* note 6 (court finds plaintiffs failed to properly plead ascertainable loss); *Randolph v. ING Life Insurance and Annuity Company*, 973 A.2d 702 at 710 (D.C. Court of Appeals 2009); *Emigrant Bank*, *supra* note 8 (court finds plaintiffs failed to properly plead cognizable injury and damages); *Delhaize America*, *supra* note 7; and *Acxiom Corporation*, *supra* note 6.

Aetna, *supra* note 22 at 7.

Identity Theft Labs, “Identity Theft Statistics 2010.” Online: <<http://www.identitytheftlabs.com/identity-theft/identity-theft-statistics-2010/>>.

Smartswipe, “Canadian credit card theft stats.” March 17, 2009. Online: <<http://www.smartswipe.ca/blog/Canadian-Credit-Card-Theft-Stats.html>>.

Emigrant Bank, *supra* note 8.

People’s United Bank and Bank of New York Mellon, *supra* note 6 at 19.

[2010] J.Q. no 11510, 2010 QCCS 5385.

Consumer Privacy Cases (Bank of America) (San Francisco City & County Super. Ct., No. JCCP 4211, 2009); *TJX Companies*, *supra* note 7.

Notice of Settlement, Union Pacific, *supra* note 6.

In Re Google Buzz User Privacy Litigation, No. 5:10-CV-00672-JW (N.D. Cal. 2010).

Notice of Settlement, Union Pacific, *supra* note 6.

Consumer Privacy Cases (Bank of America), *supra* note 32.

Class Action Complaint, *Facebook*, *supra* note 13.

Settlement Agreement, *Palmer v. Sony BMG Music Entertainment*, No. 06-CV-304178CP.

CANADIAN PRIVACY LAW REVIEW • Volume 8 • Number 2

³⁹ Under the *Fair and Accurate Credit Transaction Act*, 15 U.S.C. § 1681(g)(1), it is a violation to knowingly print more than five digits of a credit card or debit card with the expiration date on sales receipts at the point of sale.

⁴⁰ *Parker. v. Time Warner Entertainment Co.* 631 F.Supp.2d 242 (E.D.N.Y. 2009) [*Time Warner Entertainment*].

⁴¹ 47 U.S.C.A. § 2(f).

⁴² *Time Warner Entertainment, supra* note 40 at 246-247.

⁴³ *Ibid.* at 273.
