



worklaw<sup>®</sup> network

# PILCHAK COHEN & TICE, P.C.

*Attorneys Representing Management in Labor and Employment Law*

## WORKPLACE CHRONICLE

November/  
December  
2005

Inside this issue:

Making His List, Checking it Twice	1
Recent Victories for Our Clients	1
Model Social Security Privacy Policy	3
Arbitration Agreements Enforceable, but...	3

### Recent Victories for Our Clients

PC&T obtained dismissal from the Sixth Circuit Court of Appeals of an appeal from an earlier decision of the Federal district court in Detroit. The class action lawsuit had been brought by a union and some 80 employees who had been displaced when PCT's client became the successful bidder to provide services at a major public facility. The union had represented the displaced workers and had a collective bargaining agreement with the previous service vendor. PC&T successfully removed the action from Wayne County Circuit Court to federal court, and obtained summary judgment on all claims. That order will now be final with the Sixth's Circuit's dismissal of the union's appeal.



### MAKING HIS LIST, CHECKING IT TWICE

Privacy of Employee Data

#### Social Security Number Policy Required By January 1, 2006

One of the big topics at the Association of Corporate Counsel ("ACC") annual meeting in Washington D.C. this year was privacy of information. A number of states, including Michigan, have passed statutes that now require employers to guard against identity theft. Federal legislation is being drafted. Accordingly, it was not long before an employer asked PC&T if it should now officially discourage the compilation of employee names and addresses in holiday card lists. Though tempted to defer the question to the firm of Grinch & Scrooge, unfortunately the concern is real.

First, Michigan is in the forefront of protecting employee information. Recently, Michigan passed the Social Security Number Privacy Act, MCLA 445.81 et seq., that requires precautionary steps to avoid publicizing social security numbers in an employment or customer context. In particular, employers may not intentionally do any of the following with respect to employees or other individuals:

- Publicly display (including on a visible computer screen) all or more than four sequential digits of an employee's social security number ("SSN");
- Use all or more than four sequential digits of the SSN as their primary account number unless it is used in the ordinary course of business for administrative purposes;
- Visibly print all or more than four sequential digits of the SSN on any identification badge or card;

- Require an individual to use or transmit all or more than four sequential numbers of the SSN over the internet or a computer system or network unless the connection is secure or the transmission is encrypted;
- Require an individual to use or transmit all or more than four sequential numbers of the SSN to gain access to the internet website or a computer system or network unless the connection is secure or the transmission is encrypted or other identification is also required to gain access;
- Include all or more than four sequential digits of the SSN in or on any document or information mailed or otherwise sent to an individual if it is visible from outside the envelope/packaging; and
- Include all or more than four sequential digits of the SSN in any document or information mailed to a person after January 1, 2006.

**The new law requires employers to adopt policies protecting Social Security Numbers no later than January 1, 2006.**

**PC&T has a model policy in this newsletter and on our website.**

Also, the new law requires employers to adopt policies addressing these requirements by no later than January 1, 2006, and that the policy be published in a policy manual or handbook. PC&T has drafted a model policy in keeping with the requirements of this new law, a copy of which is found in this newsletter and on our website. As stated in April, 2005, Workplace Chronicle, PC&T suggests that all employers disseminate the new policy to employees as an addendum to existing

*(Continued on page 2)*

**PILCHAK COHEN & TICE, P.C.**

30500 Northwestern Hwy  
Suite 200  
Farmington Hills MI 48334-3177  
Phone: 248.626.7300  
Fax: 248.626.7305  
Email: firm@mi-employmentlaw.com

FIND US ON THE WEB AT  
[www.mi-employmentlaw.com](http://www.mi-employmentlaw.com)



**FORMS & POLICIES AVAILABLE ON  
THE PC&T WEBSITE:**

- Benefits and Detriments of Arbitration of Statutory Claims vs. Traditional Litigation
- Consent and Authorization to Release Employment Information
- Employment Application
- Fair Credit Reporting Act Forms
- Garnishee Disclosure Form
- HIPAA Authorization for Disclosure / Use of Personal Health Information
- I-9 Forms
- Policy—Wage Deductions
- Relief of Charge
- Sample CCW Memo
- Sample Certification for Users of Consumer Report
- Severance Agreement and Release of Claims
- Severance Agreement and Release of Claims (In Compliance With Older Worker Benefit Protection Act)
- WH 380/381 Forms (under FMLA guidelines)
- Social Security Privacy Policy
- Workplace Violence—Risk Factor Checklist

(Continued from page 1)  
handbooks.

There is no per se federal or Michigan “right to privacy” statute with respect to home addresses and telephone numbers. Indeed, Michigan’s “personnel file” statute, the Bullard-Plawecki Employee Right to Know Act, contemplates that contents of personnel files will at times be revealed to third parties, as it contains provisions for some removal of contents or notification of the employee upon revelations of disciplinary actions.

Despite the lack of statutory restrictions, we have been watching the developing “privacy” case-law, because it is an amorphous tort, which plaintiff-side attorneys seek to expand. In Bell v Michigan Council 25, 2005 WL 356306 (Mich App 2005) employees sued their union for not properly safeguarding the SSN’s and addresses of its members under common law principles of negligence. For a successful negligence claim, the defendant must have violated a “legal duty,” leading to injury (here, identity theft). Since the passage of the new Michigan statute, there is now unquestionably a legal duty to protect SSN’s. However, there is presently no legal duty to prevent the release of only names and addresses. However, the Bell decision contains language that a plaintiff’s attorney could rely on in future arguments: “society has a right to expect that personal information divulged in confidence...will be guarded with the utmost care” and noting that defendant was “in the best position to protect plaintiffs because it controls who has access to its membership lists.”

For those clients with operations on the west coast: California has adopted a Constitutional provision that grants all individuals (both in the private and public sector) a right to privacy. One case has extended that to the publication of addresses. In Huntingdon Life Sciences, Inc. v Stop Huntingdon Animal Cruelty, 129 Cal App 4<sup>th</sup> 1228 (2005), the Court found that an organization that advocated property damage to those conducting animal experiments could be enjoined from publishing individual’s names, addresses, and other identifying information on a website. However, the Court looked not only to the Constitutional provision, but to the tort of invasion of privacy, which requires: (1) intrusion into a private matter, (2) in a manner highly offensive to a reasonable person. A website advocating property damage obviously satisfies this. It is an open question as to whether an innocuous release of addresses or telephone numbers would result in liability, even in California.

Accordingly, the case law has crept up to a point just short of requiring employers to keep names and addresses private. However, beyond the liability and identity theft issues, there are other reasons why a company might want to discourage the creation of a written employee list: 1) the list could be used (indeed requested) by unions to organize the workforce; 2) The list could be used by competitors to recruit from the employer’s workforce; 3) The addresses could be used by stalkers, harassers or disgruntled employees for acts of mischief or worse. Accordingly, there are business reasons to adopt a policy or practice beyond strict privacy and liability issues.

The above state of affairs raises the question of whether an employer should simply publish a policy prohibiting or regulating the dissemination of addresses. Ironically, doing so has two negative implications: First, once a policy exists prohibiting the dissemination of addresses and telephone numbers, it rather dramatically strengthens the argument that there is a “duty” to safeguard addresses and telephone numbers. Second, one cannot openly cite the dangers of the list being used in a union-organizing campaign without that statement later being cited against the Company as evidence of anti-

(Continued on page 3)

(Continued from page 2)

union animus in proceedings before the National Labor Relations Board.

Thus, PC&T recommends that clients not publish a policy against dissemination of any address list. Rather, employers may take steps to prevent the creation and dissemination of employee lists via a memo to management and human resources personnel. The suggested format is as follows:

#### MEMO

To: Human Resources Personnel Management [at whatever level accomplishes this task]

From:


Re: Dissemination of Employee Information

Date:

As most people know, there is an increased sensitivity to the release of information considered personal (though perhaps not technically “private”) by individuals. As such, the company wishes to provide guidelines to personnel who may have access to employee information, during the holiday season, when requests may be made for personal information on other employees, including addresses or telephone numbers for holiday cards or party invitations:

- For Human Resources personnel at any level: It is almost never appropriate to provide information to which you have access concerning employees which is not accessible to those outside of the HR department. Confidentiality is a prime function of any Human Resource position. Thus requests for any type of information should normally be declined, unless discussed with and approved by your supervisor.
- For Managers: Creating any list of employee home addresses and telephone numbers in any business unit is to be avoided for a number of reasons:
  - Employees could be disappointed or irritated that information which they have provided to the Company has been shared;
  - It could provide a recruiting list for our competitors, and result in the loss of talent upon which you rely;
  - It provides a means for other solicitations of our employees by outsiders without knowledge by the Company, which solicitations may be merely annoying to our employees or actually harmful to the Company.

Accordingly, those in management or Human Resources must decline to create or provide any list of employee addresses or phone numbers. If a reason is needed, I recommend that you tell those making the request that

the company feels uneasy about providing personal information in the current climate, and suggest that individuals request information from the close associates among their co-workers to compile their own private lists. 

### Model Social Security Privacy Policy

Consistent with the Company’s policies on safeguarding non-public customer information, the Company recognizes that employees and others, including its customers, have privacy rights in their social security numbers in accordance with Michigan law. Accordingly, only employees with an absolute need for access to social security information will be given access to this information. Moreover, the Company treats social security numbers as confidential information. This means that the information must be kept secure in locked files and employees must have special clearance and special access codes to access the information on computers.

In those cases where authorized employees have accessed the information on their computer, under no circumstances should the information be visible to the public on the computer screen. The best way to secure the information on a computer is to limit your access to occasions when you are in a closed office or in a private area and your computer screen is not visible to those who might be passing by. The Company requires that employees shred any documents containing social security information.

Employees who access the information without proper authorization, who disclose the information or improperly dispose of documents containing social security information shall be in violation of this policy. Violations of the policy will result in discipline, up to and including discharge.

### Arbitration Agreements Enforceable, but...

Michigan’s public policy, strongly favors the use of arbitration to resolve disputes. But an arbitration provision is *not* enforceable if it is not part of a binding contract. So when is an arbitration provision enforceable, yet not a binding contract?

Many employers use personnel manuals, which state, their policies are “neither an employment agreement, nor a contract of employment” or “Personnel policies may be amended from time to time.” The intention of this language has historically been to maintain an “at will” employment relationship. But, when some employers have tried to enforce arbitration provisions, containing this disclaimer language, they have faced the argument that the

(Continued on page 4...)

(Continued from page 4)

arbitration provision is not enforceable because it is not part of a binding contract. And, Michigan courts have agreed. Stewart v Fairlane Community Mental Health Center, 225 Mich App 410, 420 (1997).

As a consequence, Michigan employers seeking to make arbitration a condition of employment and disclaim employment contracts must now take a second look at their existing policies. The analysis involves, “whether the policy overstates the avoidance of an employment contract?” If so, is your arbitration provision enforceable?

Recently, the Michigan Court of Appeals ruled that a restaurant worker who claimed he was fired after calling the police to report missing funds cannot sue under the Whistleblower Protection Act because he signed an agreement to arbitrate employment related disputes. Barna v Darden Restaurants, Inc. (November 17, 2005). The case, interpreted the restaurant's personnel policies that contained the familiar language, “Finally, I also understand this is *not a contract of employment.*”

Notwithstanding this disclaimer, the court found two important elements of the policy permitted enforcement. First, the

restaurant's personnel documents included an “*acknowledgment*” with language specifically mentioning the arbitration policy and that the employee agreed to be bound by it. Second, the acknowledgment expressly stated that the employer was equally bound by the arbitration provision. The court held arbitration could be enforced because it represented “a condition of employment.”

If arbitration is a mechanism you desire for resolving workplace disputes, double-checking your employment policies is essential. ■

Seasons Greetings  
from everyone at  
Pilchak Cohen  
& Tice, P.C.



You can find back issues of the *Workplace Chronicle* on the Web at “[www.MI-EmploymentLaw.com](http://www.MI-EmploymentLaw.com)”

PILCHAK COHEN & TICE, P.C.  
30500 NORTHWESTERN HWY., SUITE 200  
FARMINGTON HILLS MI 48334-3177