HB 319

4/29

HOUSE JUDICIARY STANDING COMMITTEE

DATE: 4/29/98 ISSUE: Amend to Amend # 1 - HB319

ASL

	YEA	NAY	PRESENT
Representative James		✓	
Vice Chair Bunde	✓		
Representative Berkowitz		✓	
Representative Croft	✓		
Representative Rokeberg		✓	
Representative Porter		✓	
Chairman Green		✓	
TOTALS:			

PASSED 2 FAILED 6

4/29

HOUSE JUDICIARY STANDING COMMITTEE

DATE: 4/29/98 ISSUE: Amend #1 - HB319

	YEA	NAY	PRESENT
Vice Chair Bunde	✓		
Representative Berkowitz		✓	
Representative Croft		✓	
Representative James	✓		
Representative Porter	✓		
Representative Rokeberg		✓	
Chairman Green	✓		
TOTALS:			

PASSED ✓ FAILED _____

4/29

HOUSE JUDICIARY STANDING COMMITTEE

DATE: 4/29/98 ISSUE: Amend #2 - HB319

	YEA	NAY	PRESENT
Vice Chair Bunde		✓	
Representative Berkowitz	✓		
Representative Croft	✓		
Representative James		✓	
Representative Porter		✓	
Representative Rokeberg		✓	
Chairman Green		✓	
TOTALS:			

PASSED 2 FAILED 6

4/29

HOUSE JUDICIARY STANDING COMMITTEE

DATE: 4/29/98 ISSUE: Amend. #3(?) HB 319

	YEA	NAY	PRESENT
Representative Rokeberg		✓	
Representative Porter		✓	
Representative James		✓	
Vice Chair Bunde		✓	
Representative Berkowitz	✓		
Representative Croft	✓		
Chairman Green		✓	
TOTALS:			

PASSED 2 FAILED 6

4/29

HOUSE JUDICIARY STANDING COMMITTEE

DATE: 4/29/98 ISSUE: Amend. #4 - HB319

	YEA	NAY	PRESENT
Vice Chair Bunde		✓	
Representative Berkowitz	✓		
Representative Croft	✓		
Representative James		✓	
Representative Porter			
Representative Rokeberg		✓	
Chairman Green		✓	
TOTALS:			

PASSED 7 FAILED ✓

4/29

HOUSE JUDICIARY STANDING COMMITTEE

DATE: 4/29/98 ISSUE: Am. #5 - HB319

	YEA	NAY	PRESENT
Vice Chair Bunde		✓	
Representative Berkowitz	✓		
Representative Croft	✓		
Representative James		✓	
Representative Porter			
Representative Rokeberg		✓	
Chairman Green	✓		
TOTALS:			

PASSED _____ FAILED ✓

4/29

HOUSE JUDICIARY STANDING COMMITTEE

DATE: 4/29/98 ISSUE: move HB 319

	YEA	NAY	PRESENT
Representative Rokeberg	✓		
Representative Porter			
Representative James	✓		
Vice Chair Bunde	✓		
Representative Berkowitz		✓	
Representative Croft		✓	
Chairman Green	✓		
TOTALS:			

PASSED ✓ FAILED _____

4/29

AMENDMENT #3

BY REPRESENTATIVE CROFT

OFFERED IN HOUSE JUDICIARY

TO CSHB 319 ( ) "B" version

Page 2, line 6, following "employer":

Insert "; or

(3) an area or compartment used to store an employee's personal belongings"

LEGAL SERVICES

DIVISION OF LEGAL AND RESEARCH SERVICES
LEGISLATIVE AFFAIRS AGENCY
STATE OF ALASKA

(907) 465-3867 or 465-2450
FAX (907) 465-2029
Mail Stop 3101

130 Seward Street, Suite 409
Juneau, Alaska 99801-2105

MEMORANDUM April 27, 1998

SUBJECT: Draft CSHB 319( ) - "B" version (Employees' expectation of privacy in employer premises)

TO: Representative Norman Rokeberg

FROM: Teresa B. Cramer
Legislative Counsel

Enclosed is the draft CS you requested. I have a few drafting comments:

1. Please see my clarification in the first sentence of sec. 23.10.450(a), that this bill is limited to expectations between an employer and the employee.

2. Expanding the definition of "employer".

In my opinion, the definition already includes private sector employers. The bill defines an employer as "a person who has one or more employees." This language is modeled after the Alaska State Human Rights Act definition, which has been applied to the private sector. The definition in your bill goes on to make clear that governmental status does not serve as an exemption from the definition of employer. That is the reason for the listing of the state, the university, the railroad, political subdivisions, and public corporations.

3. Definition of "employee" and coverage of school board members.

In the CSHB 319(L&C), there was language stating that elected officials were not to be considered **employees**. (Apparently there was some confusion about whether a school board member might be considered an **employer**. The exclusion did not address that question.) The purpose of excluding elected officials from consideration as employees was, at least in part, to protect the files of elected officials (including legislators) from disclosure to the presiding officer or the voters or whoever else might be considered the elected officer's "employer." Now that the bill contains a definition of employee, I have moved the exclusion of public officers from consideration as an employee to that definition. See Sec. 23.10.450(c)(2) subparagraph (B).

4. Protection for private phone calls and privately-owned computers.

See the new Sec. 23.10.450(b).

TC:jdr
98-270.jdr
Enclosure

0-LS1211\B
Cramer
4/27/98

CS FOR HOUSE BILL NO. 319( )

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTIETH LEGISLATURE - SECOND SESSION

BY

Offered:
Referred:

Sponsor(s): REPRESENTATIVE ROKEBERG

A BILL

FOR AN ACT ENTITLED

"An Act relating to an employee's expectation of privacy in employer premises."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:

*** Section 1.** AS 23.10 is amended by adding a new section to article 7 to read:

Sec. 23.10.450. No employee expectation of privacy in employment site. (a) In the absence of a specific written agreement to the contrary, between an employer and an employee of the employer, an employee has no expectation of privacy with respect to business premises, business equipment, and services supplied by the employer, and an employer may have reasonable access to business premises, business equipment, and services supplied by the employer to the employee. In the absence of a written agreement permitting the employee to limit the employer's access to business premises, business equipment, and services, an employee may not hinder or obstruct the employer from access to the employer's business premises, business equipment, and services, including information stored on a computer or computer network or other service supplied by the employer.

(b) This section does not waive an employee's expectation of privacy with

New Text Underlined [DELETED TEXT BRACKETED]

respect to

(1) a personal telephone call;

(2) premises or equipment, including a computer and computer information, owned by the employee but used in the employee's employment for the employer even if the equipment is connected to the employer's equipment or service for the equipment is supplied by the employer.

(c) In this section,

(1) "elected official" means the governor, the lieutenant governor, a member of the legislature, a justice or judge, or a person elected to municipal office;

(2) "employee"

(A) means a person employed by an employer and includes

(i) a permanent, seasonal, probationary, or temporary employee whether employed full-time or part-time;

(ii) an independent contractor and an employee of an independent contractor retained by the employer;

(B) does not include an elected official;

(3) "employer" means a person who has one or more employees and includes the state, the University of Alaska, the Alaska Railroad, and political subdivisions and public corporations of the state.

ALASKA STATE LEGISLATURE
House of Representatives

COMMITTEE ASSIGNMENTS:

LABOR & COMMERCE COMMITTEE, CHAIRMAN
SPECIAL COMMITTEE ON OIL & GAS, MEMBER
JUDICIARY COMMITTEE, MEMBER
CORRECTIONS BUDGET SUBCOMMITTEE, MEMBER
ADMINISTRATION BUDGET SUBCOMMITTEE ,MEMBER
HESS BUDGET SUBCOMMITTEE, MEMBER

INTERIM:
716 WEST 4TH AVENUE, SUITE 640
ANCHORAGE, AK 99501
PHONE: (907) 258-8191
FAX: (907) 258-2916

SESSION:
STATE CAPITOL
JUNEAU, AK 99801-1182
PHONE: (907) 465-4958
FAX: (907) 465-2040

Representative Norman Rokeberg

MEMORANDUM

TO: Teresa B. Cramer, Legislative Counsel

FROM: Rep. Norman Rokeberg

DATE: April 24, 1998

RE: CSHB 319 (L&C)

During the House Judiciary Committee meeting today various questions came up about CSHB 319 (L&C). The Committee would like to take this matter up again on Monday, April 27th, according to the remarks at the meeting.

1. On March 28th, I requested a legal opinion (LS-1729) on: Under current Alaska law can an employer monitor an employee's telephone, internet, or email? If so, cite statute/case law. What are the limits?

   The Committee is interested in this information and I would ask that this information be provided. The discussion in the Committee centered around whether telephone conversations would be covered under CSHB 319 (L&C) and, if they were, how to eliminate an employer's monitoring of "private" telephone conversation. Language was suggested as follows:

   > Nothing in this section is intended to eliminate the expectation of privacy as regards telephone conversations to which an individual is entitled unless specifically agreed upon by that individual employee.

   Depending on the information requested in LS-1729, this may or may not be an amendment to the current proposal.

2. Under CSHB 319 (L&C), if an employee brought a personal computer on a business premises and hooked that computer up to an employer-supplied service/data line, would the provisions of the current CSHB 319 (L&C)

apply? For example, would the employer be able to access the information on this personal computer hooked into business-owned lines and/or, in the alternative, the information flowing over the lines?

3. Please prepare a blank draft committee substitute as follows:

   a. Expand the definition of "employer" so that private employers are covered. The conversation by the committee indicated that they do not view the current language as covering both private and public sector employees and it is my intent to cover all employees, or is this unnecessary given current law?
   b. Insert a definition of "employee". This definition should include independent private contractors, independent contractors, temporary employees, regular employees, etc., when working for or with a particular employee.
   c. A local school board's members would be exempted under the "elected official" portion of CSHB 319 (L&C). However, it was pointed out at the Committee meeting that most school boards are also the actual employers of school district personnel. We need to insert language to cover this situation.
   d. If the answer to number 2 above is in the affirmative, need language to exempt privately-owned computers from employer inspection if the only connection to the employer's premises and/or service is through the employer-supplied data or telephone line.
   e. Page 1, line 11: delete "permit"; and insert "not hinder or obstruct".
   f. Page 1, line 11: delete "to have"; and insert "from".

Again, the express wish of the Committee was to review this matter again on Monday, April 27th.

cc: Representative Joe Green, Chairman
House Judiciary Committee

#3 (c)

"Nothing in this section is intended to eliminate the expectation of privacy to which an individual is entitled unless specifically agreed upon by that individual employee.

~~Also~~ remember

#1 adopt

AMENDMENT

OFFERED IN THE HOUSE **BY REP. ROKEBERG**

TO: CSHB 319 (L&C)

Page 1, line11

Delete: "permit"

Insert: "not hinder or obstruct"

Page 1, line 11

Delete: "to have"

Insert: "from"

#2

AMENDMENT

OFFERED IN THE HOUSE by Representative Berkowitz

TO: CSHB 319(L&C)

Page 1, line 4, preceding "expectation":

Delete "**No employee**"

Insert "**Employee**"

Page 1, line 5, preceding "In":

Delete "(a)"

Page 1, line 6, preceding "expectation":

Delete "no"

Insert "an"

Page 1, line 7, following the first occurrence of "employer" through page 2, line 5:

Delete all material

Insert "."

LEGAL SERVICES

DIVISION OF LEGAL AND RESEARCH SERVICES
LEGISLATIVE AFFAIRS AGENCY
STATE OF ALASKA

03-25-98P02:16 RCVD

(907) 465-3867 or 465-2450
FAX (907) 465-2029
Mail Stop 3101

130 Seward Street, Suite 409
Juneau, Alaska 99801-2105

MEMORANDUM March 25, 1998

SUBJECT: Does HB 319 violate an employee's right to privacy (Employee's expectation of privacy in an employer's premises)

TO: Representative Norman Rokeberg
Attn: Janet Seitz

FROM: Teresa B. Cramer
Legislative Counsel

You have asked whether HB 319 violates the right of privacy clause in the state constitution. Article I, sec. 22 of the Constitution of the State of Alaska reads:

> The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section.

The bill states that, absent an agreement to the contrary, an employee has no expectation of privacy with respect to an employer's premises and equipment and requires the employee to permit the employer to have reasonable access to them. The bill allows the employer and employee to enter into a specific agreement varying this general rule.

The language of the bill would appear to apply this presumption of no expectation of privacy even to housing supplied to an employee by an employer. As I discussed with Janet on the telephone, this unintended extension of the bill to a person's living quarters would be hard to defend against a constitutional challenge based on an individual's right to privacy. Amendment A.3 clarifies that the bill applies only to business premises and this memo assumes that the bill is so limited in scope.

The bill is intended to permit an employer to control the use of the employer's business premises, including use of the employer's computer equipment. Sec. 23.10.450 would preclude an employee from asserting that the employee had an expectation of privacy in material stored in the employee's work space or on the computer used by the employee at work. "Employer" is not defined in the bill. This memo assumes that both public and private employers are covered. It would be clearer for the bill to define the term.

The right to privacy has been litigated in the context of an intrusion by the government into an individual's life. In the time available to me I have not found a case applying the state's right to privacy to an interaction between private individuals without state action. The language of the right to privacy in art. I, sec. 22, does not appear to limit its scope to

governmental action. In the absence of a history of court interpretation, I cannot say with certainty how a court would rule on a challenge from an employee that a private employer had violated the employee's right to privacy. Assuming that the court would apply the same test that it uses for considering claims to invasion of privacy by the government, I believe the bill would withstand a constitutional challenge.

In Jones v. Jennings, 788 P.2d 732, (Alaska 1990), the state supreme court considered whether the personnel records of two Anchorage police officers were protected from disclosure to the plaintiff, who had filed a damage action against the officers. The court upheld the superior court's order that the records be made available to the plaintiff. In reaching this decision the court said:

> the Alaska Constitution expressly protects the right of privacy for Alaska citizens. We have discussed previously that one who asserts a right to privacy must exhibit a subjective expectation of privacy "that society is prepared to recognize as reasonable." It is plausible for an employee to expect that the details contained within his personnel file are confidential and not subject to public scrutiny. Yet we do not approach this case, and the officers' right to privacy, in a vacuum. The right to privacy is not absolute. Rather, "there must be a ... balancing of conflicting rights and interests."

Id., at 737 - 738 (citations omitted). HB 319 addresses both whether an employee can have "a subjective expectation of privacy" in the business equipment and premises of his or her employer and whether "society is prepared to recognize" that expectation as reasonable. Sec. 23.10.450 answers "no" to both questions, unless the employer and employee have a specific agreement to the contrary. Given the limitation of the bill to business premises (as opposed to residences supplied by an employer) and given that the bill requires employees to give employers only "reasonable" access to the premises and equipment used by the employer, I believe that the bill would withstand constitutional challenge.

TC:jdr:lmb
98-192.jdr

ALASKA STATE LEGISLATURE
House of Representatives

COMMITTEE ASSIGNMENTS:

LABOR & COMMERCE COMMITTEE, CHAIRMAN
SPECIAL COMMITTEE ON OIL & GAS, MEMBER
JUDICIARY COMMITTEE, MEMBER
CORRECTIONS BUDGET SUBCOMMITTEE, MEMBER
ADMINISTRATION BUDGET SUBCOMMITTEE ,MEMBER
HESS BUDGET SUBCOMMITTEE, MEMBER

INTERIM:
716 WEST 4TH AVENUE, SUITE 640
ANCHORAGE, AK 99501
PHONE: (907) 258-8191
FAX: (907) 258-2916

SESSION:
STATE CAPITOL
JUNEAU, AK 99801-1182
PHONE: (907) 465-4968
FAX: (907) 465-2040

Representative Norman Rokeberg

MEMORANDUM

TO: Representative Joe Green, Chairman
House Judiciary Committee

FROM: Representative Norman Rokeberg

DATE: March 27, 1998

RE: HB 319
An Act relating to an employee's expectation of privacy in employer premises

I would request that HB 319 be heard by the House Judiciary Committee.

Attached are the following:

a. HB 319
b. CSHB 319 (L&C)
c. Sponsor Statement
d. Sectional Analysis
e. Fiscal note (zero from Department of Law)
f. Letters of support from:
   i. Alaska State Chamber of Commerce
   ii. Alaska Miner's Association
g. State of Alaska Policy Regarding Use of Office Technologies
h. Newspaper articles concerning UAF case
i. Alaska Employment Law Letter: "E-mail and Voice Mail: Liability Waiting to Happen?"
j. November 1997 article from *PC World*, "You are being watched."
k. Legislative Council's Policy on Desktop Computer Support, Software and Hardware, Amended April 29, 1997. (see page 3 for "Confidentiality of Information on Desktop Computers" and page 6 for "Personally Owned Desktop Computers")

l. Municipality of Anchorage Operating Policy/Procedure, "Acquisition, controlled access and use of e-mail and internet services", September 10, 1997.

m. Memorandum to House Labor & Commerce Committee members dated March 27, 1998.

Thank you for your consideration of this request.

ALASKA STATE LEGISLATURE
House of Representatives

COMMITTEE ASSIGNMENTS:

LABOR & COMMERCE COMMITTEE, CHAIRMAN
SPECIAL COMMITTEE ON OIL & GAS, MEMBER
JUDICIARY COMMITTEE, MEMBER
CORRECTIONS BUDGET SUBCOMMITTEE, MEMBER
ADMINISTRATION BUDGET SUBCOMMITTEE ,MEMBER
HESS BUDGET SUBCOMMITTEE, MEMBER

INTERIM:
716 WEST 4TH AVENUE, SUITE 640
ANCHORAGE, AK 99501
PHONE: (907) 258-8191
FAX: (907) 258-2916

SESSION:
STATE CAPITOL
JUNEAU, AK 99801-1182
PHONE: (907) 465-4968
FAX: (907) 465-2040

Representative Norman Rokeberg

SPONSOR STATEMENT
COMMITTEE SUBSTITUTE FOR HOUSE BILL 319 (L&C)

An Act relating to an employee's expectation of privacy in employer premises
By Representative Norman Rokeberg

CSHB 319 (L&C) addresses a contemporary issue. With the advent of modern technology and the use of it in office places, many employees are using employer's business equipment to access the Internet and send e-mail messages. While some employers have policies in place that make the employer's policy on this use plain, many do not. CSHB 319 (L&C) would make it clear that, absent a written agreement to the contrary, an employee has no expectation of privacy on an employer's business premises.

My 1998 House District 11 survey posed the following question: Should state law allow an employer the right to regulate all employee use of employer facilities and equipment (i.e., internet, computer games, etc.)? An overwhelming majority (341) favored such a law while a minority (86) opposed.

A lawsuit involving the University of Alaska at Fairbanks brought this matter to my attention. This case involved a University employee who used his University equipment to download child pornography to a personally owned ZIP drive. This legislation would not impact this type of case since the ZIP drive was personally owned equipment. However, if all equipment involved had been owned by the University then this legislation would apply.

CSHB 319 (L&C) does permit the employee and employer to negotiate a written agreement regarding access to business premises and business equipment. It is a step towards protecting both the employer and the employee and helping each party understand the other party's rights in the areas of workplace privacy and use of business premises and business equipment.

The original version of the bill was amended in the House Labor & Commerce committee to provide that: (1) the agreements be written; (2) an employee's personal property is not covered; and (3) the legislation would apply only to business premises and business equipment (thus not covering any residential facilities provided by an employer to an employee).

I would urge your support of this legislation.

ED2:3/28/98

ALASKA STATE LEGISLATURE
House of Representatives

COMMITTEE ASSIGNMENTS:

LABOR & COMMERCE COMMITTEE, CHAIRMAN
SPECIAL COMMITTEE ON OIL & GAS, MEMBER
JUDICIARY COMMITTEE, MEMBER
CORRECTIONS BUDGET SUBCOMMITTEE, MEMBER
ADMINISTRATION BUDGET SUBCOMMITTEE, MEMBER
HESS BUDGET SUBCOMMITTEE, MEMBER

INTERIM:
716 WEST 4TH AVENUE, SUITE 640
ANCHORAGE, AK 99501
PHONE: (907) 258-8191
FAX: (907) 258-2916

SESSION:
STATE CAPITOL
JUNEAU, AK 99801-1102
PHONE: (907) 465-4968
FAX: (907) 465-2040

Representative Norman Rokeberg

SECTIONAL ANALYSIS
COMMITTEE SUBSTITUTE HOUSE BILL 319 (L&C)
By Representative Norman Rokeberg

Title: An Act relating to an employee's expectation of privacy in employer premises.

Section 1: Adds a new section to AS 23.10. New section provides that there is no expectation of privacy in an employment site. Absent a specific written agreement permitting the employee to ¨mit the employer's access to premises and equipment, an employee shall permit the employer to have access to the employer's premises and equipment. This includes information stored on a computer or computer network supplied by the employer.

States that elected officials are not employees for the purpose of this section.

Defines "elected official" and "employer".

ED2:3/27/98

FISCAL NOTE

STATE OF ALASKA
1998 LEGISLATIVE SESSION

BILL NO. HB 319

Revision Date (Note if correction)

Dept. Affected: Law

Title: An Act relating to an employee's expectation of privacy in employer premises.

BRU: Civil Division

Component: Governmental Affairs

Sponsor: Representative Rokeberg

Requester: House Labor and Commerce Committee

Component Serial No.: 2207

Expenditures/Revenues (Thousands of Dollars)

OPERATING EXPENDITURES	FY 99	FY 00	FY 01	FY 02	FY 03	FY 04
Personal Services						
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	0.0	0.0	0.0	0.0	0.0	0.0
CAPITAL EXPENDITURES						
CHANGE IN REVENUES ( )						

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type)						
TOTAL	0.0	0.0	0.0	0.0	0.0	0.0

Estimate of any current year (FY98) cost:

POSITIONS

Full-time						
Part-time						
Temporary						

ANALYSIS: *(Attach a separate page if necessary)*

HB 319 amends AS 23.10, relating to employment practices and working conditions, to add a new section concerning employee expectation of privacy with respect to premises and equipment supplied by the employer. Unless there is an specific agreement to the contrary, the bill would provide no expectation of privacy, and the employer would have reasonable access to the employer's premises and equipment, including information stored on a computer or computer network supplied by the employer.

This bill will have no fiscal impact on the Department of Law.

Prepared by: Joan M. Kasson — Phone: 465-5370

Division: Attorney General's Office — Date: 3/25/98

Approved by Commissioner: Bruce M. Botelho, Attorney General — Date: 3/25/98

Agency: Department of Law

PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE

For further distribution information, call the Governor's Legislative Office

(Rev 9/97) 98inform xls/OMB

Green

From the office of . . . Representative John J. Cowdery
State Capitol Bldg., Room 416
Juneau, AK 99801
907-465-3879 phone
907-465-2069 fax

MEMORANDUM

TO: House Judiciary Committee Members

FROM: John Cowdery J.C.

DATE: April 17, 1998

RE: House Bill 319

CC:

Notes:

We recently heard House Bill 319 in the Labor and Commerce Committee. At that time I expressed my concern that personally owned equipment in the work place may be subject, under HB 319, to search by an employer. As a specific example, I have a personal computer here in my office. Since a private line was unavailable, I am forced to connect to the internet via a state connection. Does this mean my computer is open to search by my 'employer', whomever that may be?

I am concerned situations similar to mine would fall under the purview of this legislation. The bill sponsor was eager to address my concerns and there was considerable discussion in Labor and Commerce about the best method to alleviate the problem. The bill sponsor assured me that this issue would be thoroughly reviewed in your committee.

As a former employer, I am aware that there is need of legislation of this nature. I would simply ask that you carefully consider the issue of private property in the workplace as it relates to HB 319. With this issue resolved, I will be pleased to support the bill.

Thank you for your time and consideration.

Anchorage · *Star of the North*
Chamber of Commerce

In Support of HB 319 Employee Expectation of Privacy
Anchorage Chamber of Commerce
Resolution 97/98-20

WHEREAS, the Anchorage Chamber of Commerce recognizes the importance of allowing employers to control and direct the manner in which work is accomplished in their businesses and on their premises; and

WHEREAS, employers provide equipment, tools and other materials to employees to allow those employees to perform their job duties; and

WHEREAS, in the absence of an express agreement to the contrary, employees have no right to use equipment, tools or other materials provided by their employers for their own personal purposes nor should they have an expectation of privacy with respect to any equipment, tools or other materials provided by their employers; and

WHEREAS, employers have a legitimate expectation that the equipment, tools and other materials provided to employees will be used solely for authorized business activities on behalf of the employers; and

WHEREAS, the pace of technological change has made it difficult for employers to control the proper use of equipment, tools and other materials provided to employees; and

WHEREAS, employers may feel constrained in investigating the improper use, or possible theft, of equipment, tools and other materials provided to employees for fear of invading a right of privacy employees may have; and

WHEREAS, passage of House Bill No. 319 will allow employers to have full and complete access to their own premises and equipment, including information stored on a computer or a computer network supplied by them, and will allow employers to take those actions deemed necessary to the management and operation of their businesses without fear of litigation from employees based on invasion of privacy;

NOW THEREFORE BE IT RESOLVED that the Anchorage Chamber of Commerce Board of Directors supports passage of House Bill No. 319; and

BE IT FURTHER RESOLVED that copies of this resolution be sent to the Governor and members of the Alaska Legislature.

Approved on this 3rd day of April 1998.

Joe Griffith, 1997-98 Chairman

April Jensen, President

441 West 5th Avenue, Suite 300, Anchorage, Alaska 99501-2309 (907) 272-2401 FAX (907) 272-4117
email: info@anchoragechamber.org www.anchoragechamber.org

Headquarters:
217 2nd Street, Suite 201
Juneau, Alaska 99801
(907) 586-2323 FAX 463-5515

ALASKA
★STATE★
CHAMBER
OF COMMERCE

February 27, 1998

Representative Norman Rokeberg
Alaska State Legislature
State Capitol
Juneau, Alaska 99801

Dear Representative Rokeberg:

At a meeting earlier this week, the Legislative Committee of the Alaska State Chamber of Commerce discussed the four pieces of legislation introduced by you and for which you requested our comments or position. I am able to respond to you with the following:

ASCC supports HB 319, regarding an employer's right to reasonable access to premises and equipment supplied by the employer.

We took no position on the other bills:

- HB 433, offering a tax credit to businesses for employing state residents who graduate from Alaska post-secondary education institutions
- HB 435, regarding the definition of consumer price index
- HB 458, regarding beer and wine licenses for golf courses

Generally, it is the State Chamber's practice to limit the issues we become active in each year to a specific few priorities adopted by our membership. Of the sixty-eight issues submitted by the membership this year for consideration, only twelve were adopted as priorities. The criteria for an issue to be included in our priorities is that it must be consistent with the mission and purpose of the State Chamber, and it must be of significant importance to business statewide. We believe this concentration of effort increases our effectiveness.

ASCC's Legislative Committee is responsible for monitoring all legislation and determining what action is necessary should additional issues arise that may significantly affect business. We do, therefore, appreciate your efforts to keep us informed on the issues on which you are working. We know that you are committed to strengthening Alaska's economy through economic development and that you are a friend to business. We sincerely thank you for your continuing efforts on our behalf.

Sincerely,

Pamela LaBolle

Pamela La Bolle
President

ALASKA MINERS ASSOCIATION, INC.
501 W. Northern Lights Blvd., Suite 203, Anchorage, Alaska 99503 FAX: (907) 276-7997 Telephone: (907) 276-0347

February 6, 1998

FEB - 9 1998

Honorable Norm Rokeberg
State House of Representatives
Capitol Building
Juneau, AK 99801

RE: House Bill 319, Privacy on Employer Premises

Dear Representative Rokeberg,

Thank you for the opportunity to comment on House Bill 319 which addresses the issue of employee privacy on the premises of an employer and equipment owned by an employer. The Alaska Miners Association supports HB-319 and we encourage its passage.

The appropriate relationship between the rights of an employee to privacy and the rights of an employer has been a topic of discussion for many years. However, with the expanded use of computers and E-mail the need for clearly defining this relationship has become more important. In the past, business and product security could be monitored and controlled by controlling the flow of drawings, specifications, business contacts, customers, etc. (also for the mining industry - land status, drill logs and mine plans) all of which were hard copies of the respective items.

The expanded use of computers and E-mail has significantly changed this situation. The ability of a business to safeguard its proprietary information has become more difficult and this legislation will help answer some of the potential problems that have developed.

We urge passage of House Bill 319. If we can be of further assistance in this matter please contact me.

Sincerely,

Steven C. Borell, P.E.
Executive Director

Labor Relations

MEMORANDUM

STATE OF ALASKA

DEPARTMENT OF ADMINISTRATION

To: Personnel Contacts
All Divisions
Department of Administration

Date: October 8, 1996

File No:

Phone: 465-5658

From: Mary M. Wanie
Human Resources Manager
Division of Administrative Services
Department of Administration

Subject: State Policy Regarding Use of Office Technologies

FOR IMMEDIATE DISTRIBUTION

Earlier today Commissioner Boyer issued a memorandum to all division directors concerning the referenced policy, which refines the existing policy on use of office technology. A copy of the policy is attached, which you may photocopy for further distribution.

I am asking for your assistance in distributing the policy to each employee within your span of control and assuring it is read, signed by both the employee and supervisor, and returned to the Human Resources Section for retention in the employee's record. Please check with your division director prior to distribution to avoid the possibility of duplication. In order to implement the policy as expeditiously as possible, please make every effort to have the signed policy distributed and returned within the week and all should be returned by October 18. I have also attached a computer listing of all of your division's employees as of yesterday along with their ~~supervisor's~~ name. Please return this listing certifying that each employee has been given the witness policy, along with the hard copy of the signed policy.

This memo and policy attachment has also been sent by e-mail to facilitate distribution to all personnel contacts. If you have questions, please call me.

Thank you for your help on this project as well as for your assistance on so many other projects throughout the year.

cc: Sharon Barton, Director
Division of Administrative Services

RECEIVED

OCT 10 199[illegible]

LABOR RELATIONS UNIT

State Policy Regarding
Personal Use of State Office Technologies
(Revised)

It is in the best interest of the state to encourage Alaska's state employees to learn to use the new office technologies that are fundamental to their future success as state employees. Use of technology that meets ethical standards and provides exposure, education, or experience is allowable and encouraged under this policy.

The office environment has a wide variety of technologies such as: digital telephone services (voice mail, message broadcasting, message and call forwarding), fax servers, image scanning and copying (color, reduction, enlargement, binding, collating), shared and stand-alone computers (fixed, portable), pagers (text and voice), cellular phones, data networks (local, regional, global), dial-up network facilities, Global Positioning Systems (fixed, portable), VHF and CB radios (fixed, portable), and wireless dispatched office pick-up/delivery courier services.

Use of office technologies is no different from use of any other state-provided item in the work place. Executive Branch public employees of the State of Alaska must conform to applicable Alaska statutes, orders, and codes. Recognizing the very different agency missions or division-specific needs, agencies may adopt more stringent, specific, or detailed guidelines. Reasonable use and common sense must prevail in the work place use of office technologies. All policies must contain:

Prohibited uses of office technologies (not necessarily limited to the following):

1. Use for any purposes which violate a United States or State of Alaska law or the Alaska Administrative Code.

2. Use for any commercial activities, including commercial advertising, unless specific to the charter, mission, or duties of the government agency.

3. Use for access to or distribution of indecent or obscene material or child pornography.

4. Harassing other users, computing systems, and/or damaging or altering the software components of same.

5. Use for fundraising, political campaign activities, or public relations activities not specifically related to state government activities.

6. Any activity which adversely affects the availability, confidentiality, or integrity of any office technology.

The Executive Branch Ethics Act states a public employee may not "use state time, property, equipment, or other facilities to benefit personal or financial interests" (AS 39.52.120(b)(3)). Further, "standards of ethical conduct for members of the executive branch need to distinguish between those minor and inconsequential conflicts . . . and those conflicts of interests that are substantial and material." (AS 39.52.110(a)(3))

Applicable Statutes, Administrative Orders, and Codes that you may refer to include, but are not limited to: AS 39.52, Alaska Executive Branch Ethics Act; Administrative Order #81, Nondiscrimination and Nonharrassment; Administrative Code 9 AAC 52, Alaska Executive Branch Code of Ethics; AS 39.25.160, Alaska Little Hatch Act; AS 24.60, Legislature Standards of Conduct.

The State of Alaska reserves the right to routinely monitor Internet and E-mail use by individuals and report such use to appropriate supervisors. Contents of state employees' computers are also subject to "Public Records" requests.

This policy is to be read and signed by all employees in the presence of their supervisor or agency human resources staff and filed in each employee's personnel file. The signature of the employee constitutes acknowledgment of their obligation to abide by the policy. Use of the Internet and other office technology is a revocable privilege. User accounts and password access may be withdrawn if a user violates this policy. Violations may also result in possible personnel action up to and including termination, and depending on the severity, may result in criminal prosecution and/or civil liability. After reading and signing this policy, state employees have 48 hours after the date signed to clear any material that does not conform with this policy from any office technology.

_____	_____
Signature of Employee	Signature of Witness
_____	_____
Printed Name of Employee	Printed Name of Witness
_____	_____
Department	Department
_____ _____	_____ _____
PCN Date	PCN Date

DK-AK
MB
AE

Clips from the
Fairbanks Daily News-Miner

Oct. 5 97
Sunday

Porn case sparks rights debate

By AL SLAVIN
Staff Writer

A trip through cyberspace has William Tuttle in a legal maze still under construction.

Souvenirs recovered from Tuttle's computer and disks at the University of Alaska Fairbanks have him facing criminal charges of possessing child pornography. He has lost his $42,000-a-year job at the UAF physical plant.

But just how police obtained the keepsakes—electronic images of young girls in lewd acts—has surfaced as a core issue in the case against the employee of 25 years.

A supervisor's search of Tuttle's computer system and personal disks may test the bounds of workplace privacy law as it relates to public employers and computer technology.

Tuttle's lawyer wants evidence thrown out, saying the university needed court permission to search the work station and personal computer disks. A hearing is scheduled Monday before District Judge Charles Pengilly.

"There is a serious question regarding the legality of going into someone's private belongings at work," said Tuttle's lawyer, Bill Satterberg. "The issue coming up Monday is about the right to search somebody's personal belongings. What are the rights of the employee at work?"

The university considers the computer, and anything attached to it, to be university property. It claims a supervisor identified an illegal use and turned it over to police.

Tuttle, who faces up to a year in jail, pleaded innocent July 15 to four counts of possessing child pornography. He was fired four days later.

"Obviously these two things are very inter-related," said Patty Kastelic, UAF's human resources director.

Tuttle, a 47-year-old UAF graduate, had worked at the university for 25 years. His union has appealed the firing. But Kastelic said the university stands firm.

"It was certainly inappropriate use of university equipment on university time," Kastelic said. "To my knowledge, there has never been a case like this."

A legal search?

Tuttle's world started to crumble in early June when physical plant network manager Dean Tabor installed a software program called ON-Technology's On-Guard Internet Site Manager. It allowed Tabor to monitor his employees' Internet trips.

Court files show Tabor's review indicated someone had accessed questionable sites over Tuttle's terminal. Tabor said the sites' content involved "underage pornography and male homosexuals."

Tabor checked Tuttle's computer the following day and found someone had intentionally erased the scroll, which retains the addresses of sites visited on the World Wide Web.

On June 4, Tabor again looked at Tuttle's computer. This time he copied files from the computer's hard drive. The images reportedly showed juvenile females engaged in sexual activity.

Tuttle's computer was seized along with 10 discs from a cabinet in his office. Images had also been downloaded onto the computer discs.

Tabor gave the information to the UAF Police Department and then testified when police obtained a search warrant to enter Tuttle's home. Police went looking for computer printouts but came away with pictures of a young female with balloons under her shirt and an inventory of 10 pornographic videotapes.

Tabor also identified Tuttle as the computer's primary user. Satterberg, however, said the computer was shared by several people and that Tuttle's computer password was taped to the terminal.

PLUGGED IN—The Computing and Communications' Micro Lab at the University of Alaska Fairbanks allows users to access the Internet. A criminal case against a university employee who is accused of downloading child pornography could test the limits of privacy law.

Clips from the
Fairbanks Daily News-Miner
Oct 5 97
Sunday

COMPUTER: Courts left to decide employee privacy rights

For the attorney, the issue reeks of George Orwell and Big Brother. In addition to challenging the computer and disc searches, Satterberg also questions whether Tabor had the legal authority to download them.

"They went to his office, went into his locker, took the discs that he personally bought at Fred Meyer and downloaded them," he said, "and on the basis of that went to obtain their search warrant."

That, he said, is wrong. Authorities should have first had a search warrant to pry into the computer and discs, which he compared to a purse or handbag. Should an employer be able to search those without a warrant?

"The issue isn't what you find, it's how you find it," he said.

UAF Police Chief Terry Vrabec defended the search. He said his officers consulted the state district attorney's office in Fairbanks and followed standard search warrant procedures.

"At this point, I would say that we filed everything, to the best of our knowledge, with the correct procedures," Vrabec said. "We did the best that we could within the guidelines."

New rules in the computer age

Those guidelines are based on traditional legal standards, which are now being applied to an evolving field of computer technology. The Computer Crime Division of the U.S. Department of Justice has created its own set of guidelines for local agencies to follow.

Dave Banisar, a lawyer at the Electronic Privacy Information Center, recently reviewed them. Several of his points may relate to Tuttle's case:

- Public employees are protected against unreasonable computer searches under the Fourth Amendment except for "non-investigatory, work-related intrusions" or "suspected work-related employee misfeasance."
- Individual employees may have a right to privacy that cannot be waived by a co-worker or supervisor in the same office.
- Search warrants should be obtained before computers are searched. Without one, a prosecutor should argue that the user could not have expected privacy.

Assistant District Attorney Leslie Dickson claimed, in her response to Satterberg's motion to suppress evidence, that Tuttle had no expectation of privacy. Dickson said this was evident because he downloaded information onto his own computer discs.

Under university policy, those discs—or anything else attached to an employee's work computer—become university property.

"If the university had the authority to access the discs, it certainly had the authority to decipher the contents," Dickson wrote in her court filing. One of those discs contained both work information and a piece of evidence used to charge Tuttle.

Should Tuttle have expected privacy within the university system?

Part of the answer may hinge on his relationship with his employer. Many employers now spell out just what an employee can anticipate. No one should expect privacy on their work computer unless it has been clearly established beforehand, according to one law professor.

"It's an employer's system so long as he has not created any expectations," said George Trubow, a professor of technology and privacy law at John Marshall Law School in Chicago. "Complaints about it are frequent as employees are discovering that employers are monitoring their e-mail."

A private university would not face search problems in a situation similar to UAF and Tuttle, Trubow said. A private employer is free to peruse its computer system and turn questionable items over to police.

UAF, however, falls into the "state agency" category and faces limitations instilled under the Constitution. The Fourth Amendment provides an individual with the right to be free from unreasonable searches. It also guarantees the right to be "secure in their persons, houses, papers and effects" from government intrusion.

Where now?

The Tuttle case has prompted university officials to take a closer look at access on a system of considerable size—7,500 individuals access the Internet on 5,000 network connections.

"We've just opened up Internet access to students' rooms," said Steve Smith, UAF's computer network director. "We've got another 63 modem lines coming in so people can dial in from home."

That poses another set of computer search issues. Does the university have the right to search a home computer connected to the system? Or the home itself for computer discs?

The university's ability to monitor Web site traffic is limited by the search software, which cannot search an entire network, and by a staff too few in number to track the high volume of data.

Smith said the university also has another reason for not wanting to monitor Web traffic: It does not want to be the content police.

"We treat this along the same lines as the library does with patron records in that those are confidential," he said. "We don't keep a record of what's been checked out unless it's necessary to check the system."

Smith said he didn't think he would readily turn over such records to police. "We'd probably draw the line on that and say that we have to have legal justification."

Clips from the
Fairbanks Daily News-Miner

Oct. 7 97

UAF manager tells how evidence gathered in child pornography case

By AL SLAVIN
Staff Writer

A computer network manager said Monday that two university police officers monitored another employee's Interne travels from a separate terminal in order to catch him viewing child pornography.

"They were basically waiting in my office at the monitor for a red flag to come up," said Dean Tabor, network manager for the University of Alaska Fairbanks physical plant.

When the "red flag" didn't materialize, the officers decided to seize William Tuttle's computer and some disks kept in a filing cabinet.

Tuttle was charged with four counts of possessing child pornography. But his attorney, Bill Satterberg, has challenged whether the officers had the right to search Tuttle's computer and disks without a warrant.

Tabor testified for an hour Monday during a hearing to decide whether the evidence should be suppressed. He said it was his job to monitor the capacity and activity on the physical plant's computer system.

He used a software program that not only gauged Internet traffic but also identified questionable sites with a red flag icon. Tabor said he noticed questionable sites and traced them back to a computer in Tuttle's office.

See HEARING, Page B-2

HEARING: Evidence in child porn case

Continued from Page B-1

"I viewed a couple of sites as they came by and said this is obviously not work related," Tabor said.

Tabor said one of the sites contained pornographic images of underage males and females. He contacted his supervisor, Joan Stagno, and they met with University of Alaska Fairbanks Police Chief Terry Vrabec, who was then a sergeant.

Tabor said Vrabec instructed him to monitor Tuttle's computer activity. He downloaded more images the next day and gave them to Vrabec. Tabor said Vrabec wanted to catch Tuttle in the act. Tabor had the ability to monitor images seconds after they appeared on Tuttle's screen.

Vrabec grew tired of waiting and seized the equipment from Tuttle's office, he said. They later obtained a search warrant to seize computer printouts from Tuttle's home.

The disks, Tabor said, had been attached to a university computer and are considered university property under the physical plant's computer use policy.

Tabor drafted that policy two years ago and initially suggested that employees' e-mail should be considered private. He said plant manager John Phillips vetoed that concept and decided that all communications were departmental property.

Privacy in the workplace has become a central issue in Tuttle's case.

The prosecution has argued in legal briefs that Tuttle knew others could monitor the system and could not have expected privacy.

Satterberg claims university officials needed a warrant to conduct the initial Web search. He does not believe that university officials or police had the right to seize the disks from Tuttle's personal work space or files from the computer.

Satterberg also challenged whether police had the right to download the disks, which contained additional pornographic images. The hearing is scheduled to resume Wednesday morning before Fairbanks District Judge Charles Pengilly.

ADN 10-18-97

Fired UAF carpenter says Internet porn browsing was research

The Associated Press

FAIRBANKS — A former university employee testified this week that he surfed the Internet for child pornography during work hours because he wanted to show others how easily accessible the material was.

"My curiosity took over," said William Tuttle, a former carpenter who was fired this summer for possessing child pornography at the university. "I thought, 'Good Lord, it's only six clicks away.' "

Tuttle, 47, said he was researching the topic to educate himself and two friends, a librarian and a schoolteacher. University of Alaska police arrested Tuttle in June and charged him with four counts of possession of child pornography.

Tuttle's lawyer, Bill Satterberg, has challenged whether university police had the legal authority to search a filing cabinet drawer and seize five computer discs.

Tuttle spent nearly an hour on the stand Thursday explaining why he downloaded images onto a personal storage device. He said he was trying to figure out how groups posted the pornographic images. Tuttle said he was also trying to figure out how other people jammed up the sites.

He was the final witness to testify in an evidentiary hearing that spanned three days.

Tuttle's case has sparked a legal debate over privacy expectations in the public work sector. Satterberg claims university officials overstepped their bounds by not getting a warrant to search Tuttle's office.

University officials claim they were operating under the physical plant's computer-use policy, which states that any equipment attached to a university computer is considered university property. They say this extends to disks recovered from the drawer of a filing cabinet where Tuttle kept belongings.

Tuttle said he never saw the physical plant's computer policy until the second week in June, a week after university police seized his computer.

District Judge Charles Pengilly said there are three key issues in the case. Pengilly said the first is whether the university's computer policy is valid. Acting personnel director Carolyn Chapman testified she had no proof that the policy was ever reviewed by the university's legal staff.

Pengilly said the second pivotal issue in the case is whether university police needed a warrant to search Tuttle's drawer. The third question is whether university police needed a warrant to access the disks from which the pornographic images of children were allegedly recovered.

Another oral argument is scheduled for Nov. 14.

Jerry Cramer

FAIRBANKS Daily News-Miner

IN BRIEF

LOCAL

Staff reports

Friendship Day held at Alaskaland

International Friendship Day for 1-6 p.m. Saturday at the aland Civic Center. The event, held each year since 1986, is held near the Oct. 24 anniversary of the founding of the United Nations.

The free event will feature about 20 groups each performing song, music and dance for 15 minutes. The idea is for people from a variety of countries to become more acquainted with each other.

Among the performers are the Yupik Eskimo Dancers, the Fairbanks Youth Orchestra, Ben Eielson Senior High School, and The Silver Spur Dancers.

For more information on International Friendship Day, call 452-7346.

Mini-library to open at Chatanika Lodge

Man says he was researching child porn

By AL SLAVIN
Staff Writer

A former university employee testified Thursday that he surfed the World Wide Web for child pornography during work hours because he wanted to show others how easily accessible the material really was.

"My curiosity took over," said William Tuttle, a former carpenter who was fired this summer for possessing child pornography at the university. "I thought, 'Good Lord, it's only six clicks away.'"

Tuttle, 47, said he was researching the topic in order to educate himself and two other friends, a librarian and schoolteacher. University of Alaska police arrested Tuttle in June and charged him with four counts of possession of child pornography.

Tuttle's lawyer, Bill Satterberg, has challenged whether university police had the legal authority to search a filing cabinet drawer and seize five computer discs.

Tuttle spent nearly an hour on the stand Thursday explaining why he downloaded images onto a personal storage device. He said he was trying to figure out how groups posted the pornographic images. Tuttle said he was also trying to figure out how other people jammed up the sites.

He was the final witness to testify in an evidentiary hearing that spanned three days. Tuttle said he never saw the physical plant's computer policy until the second week in June, a week after university police seized his computer.

"To tell you the truth, I didn't look at it," Tuttle said. "It was kind of after the fact."

Tuttle's case has sparked a legal debate over privacy expectations in the public work sector. Satterberg claims university officials overstepped their bounds by not getting a warrant to search Tuttle's office.

University officials claim they were operating under the physical plant's computer use policy, which states that any equipment attached to a university computer is considered university property. They believe this extends to disks recovered from the drawer of a filing cabinet where Tuttle kept belongings.

District Judge Charles Pengilly identified three key issues for Satterberg and the prosecutor, Assistant District Attorney Leslie Dickson. Pengilly said the first issue regards whether the computer policy is valid or not.

Satterberg questioned the university's acting personnel director, Carolyn Chapman, about the 2-year-old policy. Chapman said an employer has a right to provide a safe environment for employees and to monitor productivity.

But she said employees are not asked to waive their right to privacy. Chapman said she had no proof that the policy was ever reviewed by the university's legal staff.

Pengilly said the second pivotal issue in the case is whether university police needed a warrant to search Tuttle's drawer. The third and final question will decide whether university police needed a warrant to access the disks from where the pornographic images of children were allegedly recovered.

Another oral argument is scheduled for Nov. 14.

Loggers await contract

Nov. 28 97

Clips from the

Fairbanks Daily News-Miner

Computer questions

The detection and prosecution of a university employee who tapped into child pornography sites on the Internet raises some tough questions about the proper approach to workplace privacy. The university appears to have acted reasonably, but putting its actions under the legal system's very powerful microscope may help clarify some issues.

To start, District Court Judge Charles Pengilly has ruled that the searches of a university carpenter's file cabinet and the disks found in it were lawful. The incident began when a physical plant computer manager was testing a monitoring program and discovered that the carpenter appeared to be logging onto some pornographic sites while at work. The search of the cabinet was conducted without a warrant by a University of Alaska Fairbanks security official but with the consent of the carpenter's boss. Child pornography, which is illegal to possess, was discovered later on the disks. The carpenter was charged with the crime. (The propriety or wisdom of such censorship of possession, as opposed to publication, is an another entire issue in itself).

University policy clearly states that employees have no reasonable expectation of absolute privacy when they use the university's computer system. And when they are at work, their supervisors have the right (and the obligation to taxpayers) to make sure the employees are performing their duties.

However, such simple statements are easily undermined by the complexities of the real world. How does one treat, for example, computer network use by a faculty member working at home? Also, despite asserting the right to investigate anything on the system at any time, the central UAF computing center's policy is to require a search warrant when law enforcement officials ask to look into an individual's files. There is obviously a strong sense that some degree of privacy ought to be afforded people.

While all this is being sorted out, maybe the best policy is for people to view computers like they would a typewriter with carbon paper. If you don't want to chance a co-worker or supervisor stumbling across something embarrassing or illegal, then don't type it on carbon paper at work because someone might find the copies in the trash can. And think about your electronic disk files as you would paper files—if it's stored in your office, its privacy can't be guaranteed.

Pengilly's ruling wasn't a total victory for the university, though. He did note that the physical plant computer policy contained an overly broad claim, one that had university employees in other departments concerned. The policy said that its usage guidelines applied to "any computing resources connected to or used directly with the Physical Plant Information Systems." If applied elsewhere on campus, that kind of language could potentially describe computers owned personally by employees who log onto their university-supplied Internet accounts from home.

A computing policy group at UAF is talking about some of these issues and has a draft policy out for discussion. It can be read at www.uaf.edu/ua-policy.

DK/see about getting copy of opinion - I'm going to visit UA & read policy - Pl. share this w/ DIS folks THX. MB

RECEIVED

DEC 02 1997

LABOR RELATIONS UNIT

Office of the Governor Fairbanks, Alaska

Clips from the

Nov. 27 97

Fairbanks Daily News-Miner

UAF wins initial round in seizure of computer disks

By AL SLAVIN
Staff Writer

The university's right to monitor a worker's performance outweighs the worker's right to privacy when it comes to the case of a University of Alaska Fairbanks employee accused of possessing child pornography at work.

Fairbanks District Judge Charles Pengilly ruled Wednesday that computer disks were properly seized from William Tuttle's filing cabinet in UAF's physical plant and can be used at his criminal trial.

But Pengilly conceded that the issue is far from over.

"It's a critical issue of first impression and it needs to be decided by the appellate court before it can go to trial," said Pengilly, noting a lack of existing Alaska case law about computer privacy.

Tuttle also wants the issue resolved before his criminal trial on four counts of possessing child pornography. His attorney had tried to block the disks from being used as evidence, claiming they were taken during an illegal search.

"This has to be appealed because it affects so many more people than me," Tuttle said. "I just don't like being tied to the front of the train."

Pengilly called Tuttle's case the most interesting one he had come across since he began practicing law. He said existing case law required him to strike a balance between Tuttle's right to privacy and UAF's right to monitor workplace performance.

Pengilly struck down the physical plant's existing computer policy, which claims ownership of any item attached to a university computer. "The policy is simply not sufficient to justify the searches here," he said.

But the judge said the physical plant's computer system manager, Dean Tabor, was within his right to monitor Internet travels that departed from Tuttle's work station.

Tuttle, 47, was arrested in July, a month after university police seized computer disks containing child pornography from his office filing cabinet. He was subsequently fired from his carpenter's position in the school's physical plant. He claimed he was researching the sites so he could inform others how easily it could be accessed.

Tuttle said he is in arbitration with the university over his firing. He said university officials offered to remove the incident from his record and let him resign in order to avoid any more time in the spotlight.

He said university employees have offered calls of support and provided him with at least $5,000 to offset legal expenses.

See UAF

Tuttle's attorney, Bill Satterberg, described Pengilly's decision as a death knell for employee privacy in the workplace. Satterberg believes university police invaded his client's privacy when they searched the filing cabinet in Tuttle's office, which doubled as a break room for plant employees.

Clips from the
Fairbanks Daily News-Miner

Nov. 27 97

UAF: Court

Pengilly called it a "perfectly appropriate" use of the tracking system device. Tabor testified that he was reviewing the system's capacity when he noticed that someone at Tuttle' work station was visiting questionable sites.

Tabor informed his boss, John Phillips, the physical plant manager. At one point, Tabor simultaneously monitored Tuttle's Internet visits from another computer. University Police Chief Terry Vrabec waited alongside Tabor in the hopes that Tuttle would tap into a questionable site.

When that did not occur, Vrabec searched Tuttle's work area with the consent of Tabor and Phillips. Vrabec said he considered the disks, which were later found to contain pornographic images of children, to be university property. Pengilly said Tabor's suspicions were reasonable and justified him taking a closer look at computer traffic emanating from Tuttle's work station.

He also said Tabor and Phillips had "the authority to grant access for a search, a warrantless search."

Satterberg questioned the judge's ruling and noted that Phillips never testified at the evidence suppression hearings in October.

He said Tabor's monitoring violated federal eavesdropping laws that prohibit the unauthorized interception of a communication and argued that it was the equivalent of a conversation conducted over a telephone line.

Pengilly disagreed and questioned whether accessing information on the Internet was more in line with opening an encyclopedia.

Electronic Monitoring

Is monitoring e-mail or phone conversations an invasion of worker privacy or a business necessity? The answer to this question is not cut and dry, and technological advances in electronic mail systems and Internet access are further muddying the waters.

Traditionally, some employers have monitored employees' telephone conversations, citing a business need to maintain or improve standards of customer service and employee performance.

Now, employers have also begun setting guidelines on the use of electronic mail systems, justifying their right to regulate the form and content of e-mail by citing their ownership of the equipment used to transmit messages and their desire to minimize legal liability for inappropriate communications. Telephone voice-mail systems and Internet activities are other relatively new areas where employers have asserted their right to monitor worker activity.

"New technology presents new threats to privacy," according to Robert Belair, an attorney in Washington, D.C., specializing in workplace privacy issues. Both employers and employees have a lot of misconceptions about monitoring with regard to e-mail and other technological advancements, he added.

Rebecca Locketz, legal director for the American Civil Liberties Union's workplace rights project, agreed that as technology increases in the workplace, so do workers' concerns about being monitored. "We are getting more and more calls from people who are beginning to understand just how invasive this can be," she said.

Put It In Writing

Employers should have written monitoring policies, management experts suggest. Employers that do not have monitoring policies and do not inform employees that they are being monitored can face invasion-of-privacy claims, as well as wrongful termination lawsuits, according to management attorney Victor Schachter of the San Francisco law firm Schachter, Kristoff, Orenstein & Berkowitz.

Schachter stressed the importance of letting employees know up front whether they are being monitored and under what circumstances the monitoring will take place.

"Tell your employees what the rules of the game are," Belair advised. He also recommended that employers carefully examine their need to monitor employees to make sure the practice is driven by business needs and is not gratuitous.

Belair stressed that employers need to be aware of their legal rights to monitor before undertaking any type of action.

Federal, State Laws

Federal and state laws address the rights of employers to conduct, and the rights of employees to be protected from, telephone and electronic monitoring at work.

In general, state laws either mirror or exceed federal provisions. Where a state law affords greater privacy protection, it supersedes federal law. With regard to telephone monitoring, for example, federal law permits the "interception" of communications as long as one of the parties to the conversation has given consent; however, 11 states require the consent of all participating parties to make interception clearly lawful. As a means of avoiding consent problems, employers sometimes place recordings on incoming lines to tell callers they might be monitored.

In addition, the Fourth Amendment to the U.S. Constitution, which prohibits unreasonable searches and seizures and protects the privacy rights of public-sector employees, has been held to apply to instances of employee monitoring in the public sector.

Despite federal and state laws addressing monitoring, employees who feel they have been improperly monitored currently have very little recourse, Locketz lamented. The restrictions on monitoring telephone calls, for example, include exceptions for business-related calls. The business-related exception "basically swallows up the rule," she said. The determination of what is a business call is "a murky area," Locketz said.

While telephone monitoring presents several dilemmas for employers and employees, Locketz said "the tougher cases are the e-mail cases."

Most employers feel that because they supply the computers to employees, they have a right to view any electronic transmissions, Locketz said. "We would like to see some limits," she said. For one thing, the ACLU asserts that employees should be notified in advance about any e-mail monitoring, Locketz said.

An employee sending personal e-mail messages during his lunch break is on his own time and his communications are "none of the employer's business, as long as [the employee] is not improperly using the resources of the employer," she added.

1085-0058/97/$0+$1.00

This case highlights the multitude of problems that arise when individuals thought to be independent contractors are found to be employees. Under these circumstances, the employer may be held liable for back taxes and withholdings (plus any applicable penalties), overtime pay (plus liquidated damages), and unemployment compensation. Additionally, not only will the mislabeled individuals be eligible to participate in employee benefit plans and programs, but the past failure to include or count them may jeopardize the tax exempt or qualified status of those plans. Accordingly, it is always advisable to closely examine your work force to ensure that your freelancers or independent contractors are bona fide and not really employees in disguise.

Vizcaino v. Microsoft Corporation, 1996 U.S. App. (LEXIS) 26021 (October 3, 1996, 9th Cir.).

E-mail and Voice Mail: Liability Waiting to Happen?

The use of E-mail and other communication technology has exploded over the past few years. The E-mail explosion, as well as the widespread use of voice mail, has provided many advantages for business communication. Indeed, for many businesses E-mail and voice mail have become essential systems to function in the workplace and to compete in the marketplace.

E-mail and voice mail systems allow employees and employers to communicate more efficiently and quickly, thus saving time and money. With the rapid growth of telecommuting, E-mail has become to many persons an indispensable tool. Maintaining electronic networks also has allowed employers to track employee productivity, efficiency, and work quality. Employers have enjoyed these improvements in productivity and efficiency and have found that clients increasingly demand the service advantages which result from E-mail and voice mail technologies.

But use of E-mail and voice mail can pose real trouble for employers. The improper use of such systems may waste employers' resources as well as expose them to legal liability.

E-mail Monitoring and Potential for Privacy Claims. As use of E-mail has grown, so has employer monitoring of employees' E-mail communication. But E-mail monitoring can result in traps filled with privacy claims against the unwary employer.

Many states and courts have recognized that citizens have a right of privacy. Although the courts have generally sided with the employer and dismissed those E-mail lawsuits, the expenses of defending such litigation can be high.

A former employee of the Pillsbury Company recently filed a lawsuit in federal court in Pennsylvania over his claim of wrongful interception of his E-mail communication by Pillsbury. The employee received messages from his supervisor over Pillsbury's E-mail system on his computer at home. The employee responded, exchanging personal E-mail messages with his supervisor. The employee's E-mail messages concerned sales management and contained threats to "kill the backstabbing bastards" and referred to a planned company party as the "Jim Jones Koolaid affair." After intercepting the employee's E-mail, Pillsbury decided to terminate him for transmitting what it deemed to be inappropriate and unprofessional comments over the company's E-mail system.

The employee, believing that his privacy had been violated, turned to the federal court for relief. He sued the Pillsbury Company, claiming that his termination was in violation of public policy, which precluded the company from terminating him in violation of his right to privacy. The court, after evaluating Pennsylvania's privacy law, decided that the employee did not have a valid claim under the circumstances. The court determined that the employee did not have a reasonable expectation of privacy in the E-mail communication voluntarily made by him to his supervisor over Pillsbury's E-mail system. The voluntary nature of the comments, as well as the fact that no personal information about the employee was disclosed, led to a conclusion that no privacy interests were violated. Although Pillsbury was successful in defending against the lawsuit, the dispute probably could have been avoided.

At least part of the reason for the lawsuit was the fact that the employee believed his E-mail messages were private. Pillsbury apparently did not have any written policies concerning the use of its E-mail system. Moreover, it had assured its employees in an informal manner that E-mail could not be intercepted and would be kept confidential and privileged. In short, the company's failure to establish a written and consistent E-mail policy contributed to the problem.

Pillsbury is not alone. Lack of a written E-mail policy is an all too common oversight by many employers. A survey by *MacWorld*, a national computer magazine, revealed in 1993 that most companies that monitor E-mail conceal doing so and that very few have a written policy on electronic monitoring. You're asking for trouble if you do the same.

Watch Out for Voice Mail, Too! A recent case involving an office romance that was uncovered and revealed to an employee's jilted spouse shows why it is important to reduce employees' expectations of privacy and implement proper procedures for monitoring such communications. The employee sued

McDonald's for "eavesdropping" on voice mail messages he left for his lover at work.

The employee found himself in hot water when a McDonald's franchisee discovered the steamy messages and began playing them back for the employee's wife. The employee claimed that his privacy rights were violated by the surreptitious review and replay of the messages. The employee said he had been told that the code to retrieve messages from his voice mail box was unknown to anyone else, and he had assumed the contents would be kept private and confidential.

The case settled, but the lesson is still clear: draft and implement a written policy for your electronic communications systems now, including voice mail, before you find yourself in court defending a lawsuit.

A Written Policy Is a Must. The message from these cases is that it is important to diminish employees' expectations of privacy regarding E-mail and voice mail and to avoid incidents of questionable monitoring of such communication. Employers must control the privacy expectations of their employees from the very beginning by creating an explicit electronic communication policy which is explained to the employees.

When implementing an electronic communication policy, be sure to consider some essential points. First, make sure the nature of the E-mail and voice mail systems is described and that all of the employees are told that such systems are to be used for legitimate business purposes and business communication only. Second, employees must be informed that the employer reserves the right to access and disclose contents of all E-mail and voice mail messages in accordance with applicable law or when a legitimate business need arises. Finally, the policy should provide that all access without the consent of the sender or recipient of the message can be done only after obtaining executive or management approval. There may be other issues unique to an employer's business, existing communication system, or work force that need to be considered when drafting an electronic communication policy.

The most important aspect of any electronic communication policy is to state the employer's procedures and expectations as clearly as possible. Some examples include:

- E-mail is a written and electronic means of communication. The company's E-mail system consists of [describe company's E-mail capabilities, including whether the system consists of an internal E-mail system, E-mail through proprietary gateways to third parties, and/or Internet E-mail]. An employee should not transmit anything in an E-mail message, whether internal or external, that he or she would not be comfortable writing in a letter or memorandum using company letterhead.
- All E-mail and voice mail capabilities are provided to employees at the company's expense to assist internally in the conduct of company business and (if applicable) externally in communicating for legitimate business purposes.
- The company will not monitor E-mail and voice mail messages as a routine matter and will not tolerate the unauthorized access or use of them. However, the company reserves the right to access E-mail and voice mail messages and to disclose them to others. This policy also applies to password-protected messages. Any access without the consent of the sender or recipient must be done with executive or management approval.
- E-mail and voice mail may not be used for any messages that reasonably may be considered offensive, discriminatory, defamatory, disparaging, or threatening to any employee or any other person or entity. The company's policies against sexual or other harassment apply fully to the use of E-mail and voice mail.
- The E-mail and voice mail systems are provided to facilitate the company's business communications. The use of such systems for outside business ventures, to leak confidential or privileged information, or for personal, political, or religious causes is prohibited. The excessive or inappropriate use of such systems for personal business also is prohibited.
- By using the company's E-mail and voice mail systems, employees consent to this policy and the company's right to monitor and access E-mail and voice mail communication.
- Employees who misuse or abuse the E-mail and voice mail systems or policies set forth above may be subject to discipline up to, and including, discharge.

Those employers who implement a written policy, and make sure their employees know about it, help provide themselves with a basis for legal protection and, in the process, maintain good employee relations. Indeed, at least one recent study has shown that there was far greater acceptance of message monitoring among employees when they were notified about that possibility up front by their employer.

U.S. Supreme Court to Decide Numerous Workplace Issues

When the U.S. Supreme Court opened its new term on October 7 of this year, it had already granted

PC WORLD

PC World Nov 1997 v15 n11 p245(8)

You are being watched.

(monitoring employee Web use) (includes related articles on corporate intelligence tools, on staying out of trouble on the internet, and on Internet rights on the job)(Special Report: The Web and Your Business) (Internet/Web/Online Service Information)

Author

Logan, Ian

Abstract

Some corporations have started monitoring their employees' Internet use and many have even disciplined employees for improper Internet surfing. Most Internet-related job dismissals can be traced to repeated visits to adult-oriented Web sites; other reasons include shopping, gambling or chatting online. A PC World survey reveals that about 58% of employers who do monitoring do so to discourage recreational use, 47% to eliminate the downloading of pirated software and 33% to end sluggish downloads because of excessive surfing. Some companies use monitoring to prevent sexual harassment charges. Monitoring, while useful for management, can create a hostile work environment for employees. To avoid this situation, companies who monitor or block employees' Internet access should come out with a clear Internet usage policy that defines appropriate guidelines.

Full Text

Robert X was fired for downloading porn from the Web.And he's not alone. More businesses are monitoring Internet use and disciplining abusers.

"I'm afraid we have no choice," Robert's supervisor began. "You're fired."

Robert (not his real name) knew his job was on the line, but the news still came as a blow. For five years he'd worked as a technologist for a state agency. Robert had a solid reputation, a wife of 15 years, and four children. Now he had been fired for surfing the Internet.

Several months earlier, Robert had begun visiting sexually explicit Web sites after work hours. It became a habit and then an obsession. Before long, Robert's supervisor summoned him into her office and told him she knew he'd been visiting pornographic sites. She warned him that if it happened again, he could be dismissed. Within a few months, Robert was at it again--even though he was well aware of the risks. "I just couldn't control it," he says today. "With Internet access, suddenly there was this wealth of material that I could get easily--and for free."

For many organizations, access to the Internet's rich resources has come at a high price. Employers pay the cost in lost productivity, as some workers use their "free" Net access to shop, chat, pay bills, play games, or even download sexually explicit material. For employees like Robert, misuse of the Net can cost them their jobs.

Robert's story may be extreme, but it's not unique. According to a PC World survey of top executives at 200 companies, one in five firms has disciplined employees for improper Internet use--from taking away their surfing privileges to taking away their livelihood.

In fact, one-third of the companies we contacted monitor where their employees go on the Net. Another 12 percent plan to begin this kind of monitoring in the next 12 months. In addition, firms with more than 1000 employees are twice as likely to monitor than their small and midsize counterparts.

But watchful eyes aren't lurking in every corporate boardroom. More than half of the executives we surveyed are opposed to peering over their employees' cybershoulders. Their primary reason for not monitoring? Concern over employees' rights.

When it comes to Internet surveillance, corporate America is clearly divided. But better play it safe: Remember that whatever you do on the Internet--from downloading files to visiting sites to sending e-mail--someone may be watch- ing.

From Wired to Fired

Inappropriate internet use on the job is fast becoming a major problem, con- curs Richard Power, spokesperson for the Computer Security Institute, an information security consulting and training firm in San Francisco. "People are getting fired for this all the time."

Repeated visits to adult-oriented Web sites are the most common cause for Internet-related job dismissals. But employees have also been fired for shop- ping, gambling, or chatting online. In our survey, we uncovered nine companies that had fired employees for inappropriate Internet behavior. In addition, we found these notable cases:

Four employees at the Los Alamos National Laboratory in New Mexico were fired between late 1996 and early 1997 for surfing adult Web sites on the job. Ten others were disciplined during the same period for using the Net for online shopping and other personal reasons. Similar crackdowns occurred at Lawrence Livermore National Laboratory in Livermore, California, and Sandia National Laboratories in Albuquerque, New Mexico.

An employee of a Southern California aerospace engineering firm who was work- ing as a contractor for NASA was terminated earlier this year for spending too much time in an Internet forum on home repairs.

Six employees at an Electronic Data Systems site in Troy, Michigan, were fired earlier this year for abusing their Internet privileges. The discharged workers included one highly regarded systems administrator who, despite several warnings, made 15,000 visits to the same adult Web site in just one month.

Companies that monitor Net usage often have big investments to protect. To find out how their workers are using that investment, many firms rely on network surveillance software like Sequel Technology Net Access Manager or NetPartners Internet Solutions' WebSense, which can keep track of the sites people visit and the material they access. (See "I Spy: Tools for Corporate Intelligence" for an overview of Internet monitoring software.)

Ironically, by monitoring Internet use and disciplining abusers, companies contend that they're protecting employees--particularly when it comes to potential sexual harassment in the office that can arise from downloaded pornography.

The Need for Monitoring

According to our survey, nearly 58 percent of employers who monitor their staff's Internet travels do so to crack down on recreational use; 47 percent hope to put an end to downloads of pirated software; and exactly one-third want to avoid sluggish Internet connections due to recreational browsing or excessive downloads. But experts warn that the biggest problems resulting from inappropriate Internet surfing are legal liabilities.

"Most companies haven't fully realized the potential for liability [that the Internet poses]," says Albert Gidari, a partner in the Seattle law firm Perkins Coie who focuses on Internet law. For one thing, the problem of pornography in the workplace can mushroom into an expensive, embarrassing sex- ual harassment suit, Gidari adds.

Some companies use monitoring software almost exclusively for preventing charges of sexual harassment

or fostering a hostile workplace. For instance, the 6000 Internet users at National Semiconductor's worldwide offices are monitored randomly to ensure they aren't visiting adult-oriented Web sites, according to Dick Wilson, vice president of worldwide human resources for the Santa Clara, California, chip maker.

"Our MIS people take a random sampling once a month to see if any users are visiting sites that we know have offensive material," Wilson explains. "If we find an employee is going to any of these sites, we notify that person's man- ager."

Simply monitoring Internet usage isn't enough, explains Ed Cavazos, senior vice president and general counsel of Interliant, a data network/Internet ser- vice provider in Houston. A company is at risk if it doesn't clearly notify employees that downloading or viewing sexually explicit material will not be tolerated. And it could be charged with fostering a hostile-workplace environ- ment if supervisors are aware that their employees are visiting adult-oriented Web sites but fail to warn or discipline them, Cavazos adds.

Block That Site

Some organizations choose to put the brakes on Internet joyriding by blocking their employees' access to entire categories of sites. Filtering software, such as Microsystems Software's CyberPatrol Proxy or NetPartners Internet Solutions' WebSense, can prevent employees from accessing undesirable Web and FTP sites, Internet chat rooms, and newsgroups. It can also relieve companies of the unproven and time-consuming chore of monitoring.

"Blocking has been very effective for us," says Jeff Conley, supervisor of technical services for Johnson Controls, a Cape Canaveral, Florida, company that manages launch-based facilities for the U.S. Air Force, among other projects. "Our biggest issue was that employees would waste time on the Net. By blocking access to sites that fall into pornographic, political, entertain- ment, automotive, and other categories, we're ensuring that the Internet is used only for work-related reasons."

Nonetheless, according to our survey, blocking Internet sites is far less com- mon than monitoring. Less than one-fifth of the companies we surveyed block employee access to specified Web sites. Not surprisingly, the sites that most employers block contain adult material.

Is Monitoring Legal?

In most cases companies are well within their rights when they monitor or block their employees' Net access. "There are no laws on the books that can be interpreted as prohibiting an employer from watching what its employees do on the Internet," says Cavazos.

Federal law does offer employees a minimal degree of protection, though. The Electronic Communications Privacy Act generally prevents employers from monitoring personal communications, such as private phone calls, unless there is reason to believe a crime has occurred, or certain other exceptions. However, the ECPA does support an employer's right to monitor stored elec- tronic communications, such as voice-mail and e-mail messages, in order to protect its business, rights, or property. But employers do have some restric- tions in monitoring personal communications. The primary requirement: Employees must give their consent.

Consent can come in many forms, but not all of them are obvious. For example, your company's general employment policy might give the boss the right to monitor your private communications. When you agree to take the job, you con- sent to being monitored. To protect itself from potential legal challenges, though, a company should still get explicit employee consent in writing, Cavazos says.

From an employee perspective, the privacy horizon looks pretty bleak. Only Connecticut has placed limitations--albeit minimal ones--on electronic sur- veillance. Meanwhile, there is no pending legislation that would protect employees from electronic observation, according to Lewis Maltby, director of the American Civil Liberties Union's Workplace Rights Office in Princeton, New Jersey. What's more, according to our phone survey, nearly 14 percent of com- panies that monitor haven't told employees about the practice.

And large com- panies were much less likely to tell their employees that they were being watched.

The Big Brother Syndrome

When a company monitors its employees' use of the Internet, the result can be a fearful work environment. "I've worried from time to time that I might accidentally go to an inappropriate Web site, and it would show up on my records," says Donald B. Ward, a technician at a federal government facility in Gaithersburg, Maryland.

"There are a lot of clever Web site operators out there who can make their site show up in an Internet search, even though the site might have nothing to do with what you're researching. If you go to one of those sites and it turns out to be adult oriented, you're in complete violation of the Internet policy for our agency and could even be fired. Luckily," Ward adds, "people are reasonable here. But still, it makes you cautious."

When you give employees the freedom to surf the Internet without the specter of surveillance, they may be more productive in the long run, argues Mike God- win, staff counsel for the Electronic Frontier Foundation. This San Francis- co-based civil liberties group advocates privacy in the workplace. "Some employers have a puritanical streak that makes them feel monitoring is justified," Godwin says. "But most people don't want to work for employers like that."

"Unproductive surfing fades as people become more Internet savvy," adds Mary J. Cronin, the author of Doing Business on the Internet (Van Nostrand Rein- hold, 1994, 800/842-3636). "With every new technology, there's a learning curve, and an important part of that curve is exploration. With the Internet," says Cronin, "users often surf around to get a sense of what the whole Internet universe is all about. But eventually, most people settle down and get back to work."

Monitoring may prevent Internet abuses, but companies should still be cautious. Say a company tries to prevent Net misuse by telling its employees that it's monitoring their Internet activities but then fails to do so. In that instance, the company runs a greater risk of exposing itself to liability claims than if it never said it would monitor at all, says attorney Cavazos.

"If you say you monitor but don't, and an employee does something illicit on the Internet or in their e-mail, you might have trouble proving that you didn't know about it," Cavazos explains.

Aside from the added responsibility, monitoring employees on the Internet requires time, personnel, and other resources. In our telephone survey, slightly more than half the executives we interviewed are personally opposed to monitoring Internet usage, compared to just over one-third who say they are in favor. The primary reason for opposing Net monitoring is concern about employee privacy. Some also argue that the demands of monitoring far exceed the benefits.

"I don't monitor Internet usage for two reasons," says Scott Paddock, manager of PC Brokers, a computer value-added reseller in Denver. "First, I trust my employees; that's why they work for me. If there were to be any problems with an employee, those problems would present themselves without the need for me to get involved in cloak-and-dagger shenanigans. And second, if I spent time monitoring their Web usage, I would be just as guilty of wasting time as my behavior implies they are," says Paddock.

Making Internet Policies

Whether a company decides to monitor or block its employees' Internet access, experts agree that it should always have an Internet usage policy in place. Such a policy offers guidelines for appropriate behavior when personnel are using the employer's computers and communications resources.

"The best way to defend yourself against potential liability is often a clearly written, well-distributed Internet policy that describes the do's and don'ts," says attorney Cavazos. He recommends that employers make the finished policy part of every new employee's orientation, put it into an employee hand- book, and post it

on the company intranet. Do whatever you have to do to make sure everyone knows the policy, he adds.

It's not enough to put a policy in place; it must also be reevaluated periodically. "I review all the HR guidelines, including our Internet policy, on a quarterly basis," says Coeta Chambers, an attorney for the human resources department of Intel Corporation in Santa Clara, California. "With technology changing as fast as it does, it's important to make sure our guidelines keep up with those changes."

Some argue that the best way to keep employees out of trouble is to give them guidelines, treat them with respect, and use monitoring data only if neces- sary.

"We don't specifically monitor individuals, though we do have network monitor- ing tools," says Paul Swortz, a spokesperson for The Boeing Company, the air- craft manufacturer in Seattle. Boeing uses the data only if there's a need to investigate a complaint. "We trust employees to use common sense when working with company resources, and the Internet isn't any different from any other company resource," explains Swortz.

Making Internet Policies

Whether a company decides to monitor or block its employees' Internet access, experts agree that it should always have an Internet usage policy in place. Such a policy offers guidelines for appropriate behavior when personnel are using the employer's computers and communications resources.

"The best way to defend yourself against potential liability is often a clearly written, well-distributed Internet policy that describes the do's and don'ts," says attorney Cavazos. He recommends that employers make the finished policy part of every new employee's orientation, put it into an employee hand- book, and post it on the company intranet. Do whatever you have to do to make sure everyone knows the policy, he adds.

It's not enough to put a policy in place; it must also be reevaluated periodically. "I review all the HR guidelines, including our Internet policy, on a quarterly basis," says Coeta Chambers, an attorney for the human resources department of Intel Corporation in Santa Clara, California. "With technology changing as fast as it does, it's important to make sure our guidelines keep up with those changes."

Some argue that the best way to keep employees out of trouble is to give them guidelines, treat them with respect, and use monitoring data only if neces- sary.

"We don't specifically monitor individuals, though we do have network monitor- ing tools," says Paul Swortz, a spokesperson for The Boeing Company, the air- craft manufacturer in Seattle. Boeing uses the data only if there's a need to investigate a complaint. "We trust employees to use common sense when working with company resources, and the Internet isn't any different from any other company resource," explains Swortz.

Good Net Behavior Begins at Home

Boeing's rational approach to curbing Internet excess on the job takes every- thing into consideration--except for the irrational. The Internet is an unruly, ungoverned, amorphous technology that transmits everything from the useful and informative to the illicit and illegal directly onto computer screens throughout corporate America. That said, there are simply no easy ans- wers for how to foresee, prevent, or handle a situation in which a trusted, valuable, long-term employee loses control in cyberspace.

"I was ashamed of what I'd done, but I also feel I was treated harshly," says Robert, the technologist who was fired as a result of his Internet misdeeds. "My supervisors wanted to make an example of me." Following his dismissal, Robert was unemployed for three months.

And then, out of nowhere--a job offer. He's been at the job for several months now, and claims that his urge to surf for adult materials on the Internet is fully under control.

Ultimately, Robert's experience offers lessons for employees and bosses alike. For workers, Robert's firing is a reminder that the PC on your desk, just like the telephone beside it, is a business tool paid for by the

company.

"You wouldn't make a lot of long-distance personal calls at work and not expect anyone to notice or care, so why should using the Internet be any dif- ferent?" says Ward, the federal employee who fears he may accidentally visit an inappropriate Web site. If you have personal reasons for being on the Net, Ward adds, do it somewhere else--at home, at an Internet cafe, or at the pub- lic library.

For employers, Robert's story underscores the need for a firm Internet usage policy, according to Computer Security Institute's Power. "The most economi- cal, effective solution to this whole problem is actually rather simple," he says. "Make sure your users understand that you can see where they've been on the Internet, and that their actions online can have consequences--including dismissal. Then, make sure they're reminded of this on a regular basis." You won't entirely prevent Internet abuse, Power says, but it's a good start.

RELATED ARTICLE: Your Internet Rights on the Job

Scenario 1

Nobody told you that your Internet use in the office was being monitored. Now you've been warned you'll be fired if you use the Internet for recreational surfing again. What are your rights?

Bottom Line When you're using your office computer, you have virtually no rights. You'd have a tough time convincing a court that the boss invaded your privacy by monitoring your use of the company PC on company time. You should probably be grateful you got a warning.

Scenario 2

Your employees are abusing their Internet privileges, but you don't have an Internet usage policy. What do you do?

Bottom Line Although the law isn't fully developed in this area, courts are taking a straightforward approach: If it's a company computer, the company can control the way it's used. You don't need an Internet usage policy to prevent inappropriate use of your company computers. To protect yourself in the future, distribute an Internet policy to your employees as soon as possible.

Scenario 3

Employee John Doe downloads adult material to his PC at work, and employee Jane Smith sees it. Smith then proceeds to sue the company for sexual harass- ment. As the employer, are you liable?

Bottom Line Whether it comes from the Internet or from a magazine, adult material simply has no place in the office. So Smith could certainly sue the company for making her work in a sexually hostile environment.

The best defense is for the company to have an Internet usage policy that prohibits visits to adult sites. (Of course, you have to follow through. If someone is looking at adult material in the office, you must at least send the offending employee a written reprimand.) If the company lacks a strict Internet policy, though, Smith could prevail in court.

RELATED ARTICLE: Playing it Safe: Staying Out of Trouble on the Net

Employer

* Create a usage policy that prohibits viewing adult or other controversial sites; copyright infringement; and all unlawful and offensive communications (including e-mail).

* Distribute written or electronic copies of the policy to all employees and update it regularly.

* Inform your employees if you plan to monitor their Net usage. Don't claim to be monitoring unless you really plan to do it.

* Consider letting employees surf the Web on their own time, if they stay within guidelines.

Employee

* Ask whether your company has a written Internet policy.

* If your employer doesn't have a policy, play it safe: Do your recreational surfing from home.

* Never download or view material at work that others could deem offensive.

* Never discuss confidential or personal matters via your company's e-mail system.

RELATED ARTICLE: I Spy: Tools for Corporate Intelligence

The marketing department has gone Web-happy. Your administrative assistant reboots the computer every time you pass by. Ever since everyone in the com- pany got full Internet access, production has slowed to a crawl. You don't need to be a CIA agent to figure out that people are wasting time on the Net. What do you do? It may be time to invest in Internet surveillance software.

Gothcha! Surveillance programs perform two key functions: monitoring what employees do on the Net, and blocking access to specified sites. Some programs focus on monitoring, which is useful for documenting violations of your com- pany's Internet policy. Others excel at blocking--good if you already know what you want to make off-limits. But the software is expensive--from $995 to $5000--and complicated to set up. Most require Windows NT Server software, and some need to be integrated with proxy servers from Microsoft or Netscape. It's a job best left to network administrators.

What you watch If your primary aim is monitoring, you'll want software that tracks a variety of Net activities, like Web site visits, file transfers, and source and destination e-mail addresses. And if you've been suffering Internet slowdowns, tracking the amount of data each user downloads can tell you who's hogging all the bandwidth. Once the program logs the information, you'll need it to produce reports that make the data easy to understand. For example, Sequel Technology Net Access Manager not only provides its own reporting tools but also lets you create custom reports using any database reporting tool you choose.

Getting to know you Check out how the program tracks users. Most identify them by IP address, but some use network log-in. Log-ins are usually best--they let the IS department identify that the visitor to the Playboy site was Joe Mil- ler, rather than machine 1.160.10.240. Some programs can identify groups of users--useful if, say, you want to prevent just the accounting department from surfing the Internet.

Lists of Evils If you want to restrict employee access to the Net, look for a program that comes with a database of questionable sites organized by category--adult, politics, entertainment, and so on. You'll want to be able to customize the database with your own forbidden sites, and block sites by both URL and IP address. (Obviously, it's easy to ban access to a Web site if you know its URL, but some sites are known only by IP address.) And because the Net changes by the minute, you'll want to be able to update the database fre- quently--at least once a week.

Final Words To prevent a flood of calls to your company's tech support staff, make sure that a suitable message is sent to your employees when their access is blocked. Perhaps you could flash across their screens: 'Sorry--session terminated with extreme prejudice. Signed, Corporate Intelligence Agency.'

RELATED ARTICLE: Other Legal Minefields

Pornography isn't the only Internet abuse that should flash a warning light to employers. Copyright violation

is another potential minefield for businesses that provide their employees with Net access, warns Gidari.

"You might have an overzealous employee posting false information on the Internet about your competitors; that's defamation," Gidari says. Another example: "You might even have some employees running an illegal betting opera- tion over the Internet. In other words," he says, "there are lots of ways an employer can be held liable for something an employee does on the Internet."

According to several sources interviewed for this article, there haven't been any cases in which an employer was held directly responsible for an employee's cyberbehavior--yet. Still, observers say, it's only a matter of time.

Topic

Internet/Web Technology Application

Record #

19 906 647

Legislative Council

Policy on Desktop Computer Support, Software and Hardware
Amended April 29, 1997

Section 1. Introduction

Purpose

The best computing industry practices indicate that the Alaska State Legislature can achieve two benefits by implementing strong desktop computing standards: (1) minimize the costs to support desktop computers; and (2) provide efficient management of the desktop computing environment.

Implementing desktop computing standards will reduce the number of desktop computer platforms, operating systems, hardware manufacturers, applications and varied computing services that the Legislative Affairs Agency (Agency) must support. By reducing the variety of technologies and services it must support, the Agency can better manage the desktop computing environment and provide streamlined and improved support services to the Alaska State Legislature.

Background

On January 31, 1997 the Legislative Council Chair appointed the Subcommittee on Information Services (Subcommittee on IS) to review the Information Services function of the Agency and make recommendations for improving its services.

On April 29, 1997 the Subcommittee on Information Services recommended that the Legislative Council (Council) adopt new desktop computer policies, standards and an implementation plan. The Council subsequently adopted the Subcommittee's recommendations.

Desktop Computer Standards Policy

The Legislative Council shall establish, implement, enforce, review and update policies and standards for the desktop computer systems assigned to Legislators' Offices and legislative committees, including commissions and task forces. A yearly review of policies and standards is recommended.

Subcommittee on Information Services (Subcommittee on IS)

At its discretion, the Legislative Council Chair may appoint a Subcommittee on IS to review and recommend Information Services (IS) policies and standards to the Council for adoption or amendment.

Legislator's Offices and Legislative Committees, Including Commissions and Task Forces

The provisions of this policy apply to Legislators' Offices and legislative committees, including commissions and task forces. However, the provisions of this policy do not apply to the Division

of Legislative Audit and the Division of Legislative Finance.

Legislative Affairs Agency and Other Legislative Entities
Unless specifically provided otherwise, the provisions of Sections 2. - 5. of this policy do not apply to the Legislative Affairs Agency, the Chief Clerk's Office, the Senate Secretary's Office, the House and Senate Records Offices, the Ombudsman's Office and other entities requiring desktop computer support services from the Agency.

For these offices, the Agency shall establish, implement, enforce, review and update more comprehensive policies and standards for the complete legislative computing environment including the mainframe, networking foundation, desktop computers and all computer support services. The Agency will integrate the desktop computer policies and standards, as adopted herein by the Council, into policies and standards encompassing the complete legislative computing environment.

Section 2. Support Services for Desktop Computers

Purchasing Authority for Desktop Computer Systems
Only Legislators and legislative committees, including commissions and task forces, with funding authority may purchase desktop computer systems for Legislators' Offices and legislative committees, including commissions and task forces. The Agency is not budgeted to purchase desktop computer systems for Legislator's Offices and legislative committees, including commissions and task forces, the Division of Legislative Audit, the Division of Legislative Finance and other legislative entities not part of the nonpartisan Agency budget.

Procurement
The Agency shall procure all desktop computer software and hardware for the Alaska State Legislature, except for the Legislative Budget and Audit component entities which may optionally request the Agency to procure desktop computer software and hardware. All desktop computer software and hardware procured shall comply with the standards of this policy.

Authorization to purchase desktop software and/or hardware shall be in writing and must clearly identify the source of funding. The Agency's procurement procedures for desktop computer software and hardware shall comply with the procurement procedures adopted by the Council. Procurement shall include working with the requestor, obtaining information from vendors, selecting vendors, issuing purchase orders, tracking orders, receiving orders, creating inventory records and processing bills.

Management
All IS projects and support services shall integrate standard desktop software and hardware.

Network Connectivity
The Agency shall provide the Local Area Network (LAN), Wide Area Network (WAN) and

mainframe environments for connecting desktop computer systems. Only standard desktop systems will be connected to the network.

Programming
Only the Agency may provide for software programming for desktop computer systems.

Maintenance
The Agency shall provide for all software and hardware maintenance of desktop computer systems.

Support Services
The Agency shall perform services in support of desktop computer systems, including:

- Help Desk Management
- Problem Management
- Trouble-Shooting Support
- Software Configuration
- Session Start-Up and Wrap-Up
- Training
- Manuals and User Guides
- Software and Hardware Inventory
- Consultations

Confidentiality of Information on Desktop Computers
In accordance with the Public Records Policy regarding Legislators' records adopted by the Legislative Council on March 14, 1997, the Agency shall treat all documents, files and data on Legislators' desktop computer systems as confidential information.

Section 3. Standard Desktop Computer Software

Standard Desktop Software

1. Operating System: MS Windows 95
2. Application Suite: MS Office 95, Standard Edition (MS Word, Excel and PowerPoint)
3. Calendaring and Appointment Scheduling: Now Up-to-Date
4. Database Maintenance: Claris FileMaker Pro
5. Page Layout and Newsletter Design: Adobe PageMaker
6. Electronic Mail: Lotus cc:Mail
7. Network Based Database and Document Research: Folio Bound Views
8. Internet Web Browser: Netscape Navigator
9. POMS Processing: POMS95
10. Special Purpose Applications: Only as approved by the Council
11. Network Client: Netware Client32

Desktop Software Version Currency
The Agency shall work with the Council to establish an appropriate version of each software application to install on all desktop systems.

Assignment of Desktop Computer Software
The Chairs of the Rules Committees or Presiding Officers, as appropriate, shall assign standard desktop computer software applications to Legislators' Offices and legislative committees, including commissions and task forces. Each desktop computer will receive only the specific software packages as assigned.

Installation of Desktop Software
In compliance with the assignment of desktop software and software copyright protection provisions of this policy, the Agency shall install all software on all desktop computer systems. The Agency shall install only standard software, except in situations when the Agency determines that nonstandard software is necessary to keep desktop systems productive.

Software Copyright Protection
All software installations shall comply with all requirements of applicable copyright agreements and federal copyright laws. Software may not be copied by any Legislator or legislative employee in violation of copyright agreements or federal copyright laws.

Section 4. Standard Desktop Computer Hardware

Standard Desktop Hardware
1. The standard desktop computer system shall be MS Windows 95 compatible.
2. The Agency shall purchase desktop computer systems from a single manufacturer.
3. The standard desktop printer shall be the Hewlett-Packard 5M.
4. The Council has adopted a four-year plan to replace the Macintosh platform and personally owned desktop computer systems with standard systems. During calendar year 1997, all non-PowerMac Macintosh and DOS based computer systems shall be replaced. In 1998, the PowerMac 6100 systems shall be replaced. In 1999, the remaining PowerMac computers shall be replaced. In 2000, all personally owned desktop computers shall be replaced.

Assignment of Desktop Hardware
The Chairs of the Rules Committees or Presiding Officers, as appropriate, shall assign only standard desktop computer equipment to Legislators' Offices, legislative offices and committees, including commissions and task forces.

Installation of Desktop Hardware
In compliance with the assignment of desktop hardware provisions of this policy, the Agency shall install only standard desktop computer hardware.

Maintenance of Desktop Hardware

The Agency shall maintain all standard desktop hardware covered under this policy, including parts inventories and maintenance manuals. To minimize downtime, the Agency shall maintain an inventory of spare desktop equipment to replace production equipment in need of repair. Replacement hardware shall be similar in capabilities to equipment replaced. When necessary, the Agency shall solicit outside maintenance support for component repair.

Returned Desktop Hardware

Prior to redistribution, the Agency shall destroy all documents, files and data left on all desktop computer equipment returned to the Agency. Legislators not returning to the Alaska State Legislature shall return all assigned desktop computer equipment to the Agency no later than December 31 of the year prior to the start of the next legislative session.

Section 5. Temporary Support of Nonstandard Desktop Software and Hardware

Notwithstanding provisions in Sections 1. - 4. of this policy, the Agency shall provide temporary desktop computer support for certain nonstandard software and hardware until they are phased out. When all of the nonstandard desktop computer systems are replaced, Section 5. or the applicable subsections of this policy may be deleted.

Requests and Conditions for Support for Nonstandard Desktop Computer Software and Hardware

Support for nonstandard desktop computer software and hardware is discouraged because doing so contradicts the purpose of implementing standard software and hardware.

Requests for the Agency to acquire, install and/or support nonstandard desktop computer software, including special purpose applications, and hardware must be submitted in writing to the Council Chair.

Only as approved by the Council Chair, and as schedule and technical abilities permit, the Agency shall use its best effort to provide support services for nonstandard software and hardware. Support of nonstandard systems will not be allowed to interfere with support for standard systems. The Agency is not required to maintain technical proficiency in nonstandard software or hardware.

Examples of Nonstandard Desktop Software

1. MS Windows 3.1
2. MS Windows NT
3. MS Office 97
4. Personally owned software
5. Software purchased using Legislator's allowance accounts
6. All freeware and shareware
7. Demonstration software
8. Software not purchased in compliance with the procurement provision

9. Software not in compliance with the assignment of desktop software provision
10. Software not in compliance with the installation of desktop software provision
11. Software not in compliance with the software copyright protection provision

Examples of Nonstandard Desktop Hardware

1. Personally owned desktop hardware
2. Hardware purchased using Legislator's allowance accounts
3. Hardware not purchased in compliance with the procurement provision
4. Hardware not in compliance with the assignment of desktop hardware provision
5. Hardware not in compliance with the installation of desktop hardware provision

Macintosh Desktop Computers

The Agency shall support desktop systems installed before May 1, 1997.

Existing Desktop Software Applications

The Agency shall support desktop software applications installed before May 1, 1997.

Existing Desktop Software Application Versions

The Agency shall support desktop software application versions installed before May 1, 1997.

Existing Desktop Printers

The Agency shall support desktop printers installed before May 1, 1997.

Personally Owned Desktop Computers

The Agency shall support personally owned desktop computer systems until such time as they are replaced with standard systems. The Agency shall review each personally owned desktop computer before connecting it to the network and may restrict the connection if the system is determined to be incompatible with the network. Support for standard desktop computer software and hardware shall take precedence over personally owned systems.

MUNICIPALITY OF ANCHORAGE OPERATING POLICY/PROCEDURE	P&P No. 16-3	Page 1 of 5
	Effective Date	
Subject: ACQUISITION, CONTROLLED ACCESS AND USE OF E-MAIL AND INTERNET SERVICES	Supercedes No. 16-3	Dated November 26, 1996
	Approved by: September 10, 1997	

1. PURPOSE

To establish policy for gaining access to, and controlling the use of, Municipality-provided Internet services.

2. POLICY

It is a policy of the Municipality of Anchorage to provide Internet services for the authorized use of persons in positions determined to need them to more cost-effectively conduct official Municipal business.

3. ORGANIZATIONS AFFECTED

Any Municipal agency with specific requirements that justify the use of Internet services in daily operations, special circumstances or both.

4. REFERENCES

Policy and Procedure 28-1, Information Resource Management.

5. DEFINITIONS:

External Computer System - Any computer system not a part of the Municipal Network.

Firewall - Protection device between the Internet and the Municipal Networks. Prevents unauthorized access to Municipal systems

Internet - For purposes of this P&P the Internet is defined as interactive distribution and access of Transmission Control Protocol/Internet Protocol (TCP/IP) services such as File Transfer Protocol (FTP), Gopher, Usenet or World Wide Web (WWW).

Internet Services - For the purposes of this policy and procedure, Internet services include:

External E-Mail - The transmission of electronic messages to persons or organizations other than in-house electronic mail (in MS Mail an "SMTP" address is an external address) to include Mailing Lists.

Internal E-Mail - The transmission of electronic messages to persons employed by the Municipality of Anchorage.

World Wide Web - The use of Internet web browsers/crawlers to access hypertext documents on external computer systems.

File Transfer - The use of File Transfer Protocol (FTP) or Gopher to retrieve documents from external computer systems.

Newsgroups - Subject specific discussion forums delivered via a universal feeder network called Usenet.

Authorized use - Use where there is a documented, official need to conduct correspondence and/or research pertinent to the Municipality.

Post-it® Fax Note 7671 | Date | # of pages ▶
To JANET | From Bev Granade
Co./Dept. | Co.
Phone # 465-6547 | Phone # 343-4554
Fax # 907-465-2040 | Fax #

6. RESPONSIBILITIES:

Each Department Director, Utility Manager and Executive Manager will:

a. Be responsible for identifying and selecting the persons/positions within their area that require the use of Internet services, to include the specific services to which the position/person needs access (i.e., those persons responsible for updating the Municipal homepage).

b. Annually review, recertify and budget for each position requiring access.

c. Monitor usage reports and eliminate unauthorized use.

d. Ensure that usage of internal and external e-mail does not circumvent established correspondence routing procedures.

e. Where abuse or misuse is suspected, contact Employee Relations

The Management Information Systems Department will:

a. Maintain the master data base of all users of Internet access provided by the Municipality, and will provide a copy to the Office of Management and Budget.

b. Validate the list annually with each Department Director and Utility Manager.

c. Periodically review customer requirements and compare them to local Internet service provider capabilities and prices to determine if the Municipality is receiving the best value for service provided.

d. Establish a firewall to prevent unauthorized direct access of Municipal assets from outside of the Municipal network.

e. Monitor use and notify Departments of excessive or inappropriate use (i.e., attempts to load files directly to the server, use time significantly higher than anticipated, or attempts to bypass access-restricting software).

f. Provide virus check software for all users.

Each Employee will:

a. Appropriately use Internet services:

Internet capability is like any other instrument of business (i.e., telephone, copier, fax) and is intended to be used for the benefit of the Municipality of Anchorage with due thought and prudence. Inappropriate and/or unauthorized use may result in disciplinary action up to and including termination. (See AMC 3.30.091).

(1) E-Mail may be used to send formal and informal municipal business messages and for exchanging attached documents. Care should be exercised in the use of E-Mail because the communication is easily forwarded by the recipient and may go to addresses other than those originally intended. As an example, consider that a message to an colleague in another city could be forwarded to the editor of a trade journal. You should consider your audience as wider than your addressees. Also, be aware that E-Mail has the same legal status as any hard-copy document. **The use of the Municipal address is analogous to using Municipal letterhead stationery.**

(2) World Wide Web services may be used to conduct official Municipal business research. It is not to be used for personal research. Consider the Web as you would a library. Where it may be appropriate to research building codes as part of official duties, it may be inappropriate to be reading hobby magazines as part of official duties. Access-

restricting software may be used to block access to inappropriate sites, but it is incumbent upon the individual to use the Internet access responsibly.

(3) File transfer is a remarkably fast means of getting documents from an external location onto your computer in a form that can be used in other documents (i.e., ascii text versus retyping). It also has a hazard in that executable files (i.e., EXE, COM, BAT and CMD) may contain viruses. Do not download files directly to the network servers. Load files to your personal hard drive (C:) and then run a virus check on the file.

(4) Due to their unmoderated nature, newsgroups are among the least effective means of research. They do have value however, and should be used when needed to conduct official Municipal business research. However, as with the World Wide Web, some usenet newsgroups contain material that is inappropriate to the Municipal work environment. Access-restricting software will be used to block access to inappropriate newsgroups, but it is incumbent upon the individual to use the Internet access responsibly.

(5) All users should become familiar with Net Etiquette, sometimes called netiquette. As an example, it is considered impolite to SHOUT (all caps). The Municipality is judged on the behavior of its employees. Consider yourself Anchorage's ambassadors to cyberspace.

b. Appropriately use Internal E-Mail:

Internal e-mail is like any other form of Municipal memorandum and is intended to be used in the same manner as established correspondence routing procedures. Care should be exercised in the use of E-Mail because the communication is easily forwarded by the recipient and may go to addresses other than those originally intended.

7. PROCEDURES:

For the acquisition of Internet service (beyond External E-Mail capability):

a. An MOA Internet Request Form (96-002) (Attachment A) will be completed.

b. The form will be routed through the process described in Attachment B.

8. ANNUAL REVIEW DATE / LEAD AGENCY REVIEW AGENCY:

The Management Information Systems Department will review this document during July of each year for any needed revision.

MIS # _____

MOA Internet / E-Mail Request Form

The following is a short checklist to determine if your computer is capable of running the software required to access the Internet. If you answer no to any question, or if you need help answering the questions, please contact the MOA MISD help desk at 343-6824.

Checklist

Do you have a 486 or faster PC? or a 68030 or faster model Macintosh?	☐ Yes ☐ No ☐ Yes ☐ No
Are you currently connected to the MOA Network?	☐ Yes ☐ No
Do you have at least 60 MB of free space on your hard drive?	☐ Yes ☐ No
Do you have at least 16 MB of memory (RAM)?	☐ Yes ☐ No

Does your PC have one of the following Operating Systems?

Windows 95 ☐ Windows NT ☐
Macintosh 7.X ☐
Windows for Workgroups ☐

MISD Information Center Use Only **Consultant**_____

Notes: _____

Organizational Budget Code_____ _____

What is your business objective(s) for Internet access? (Attach explanation if necessary)

_____

_____

_____

_____

I read, understand, and agree to abide by the MOA policy and procedure (16-3) governing MOA employee use of the Internet.

_____ _____

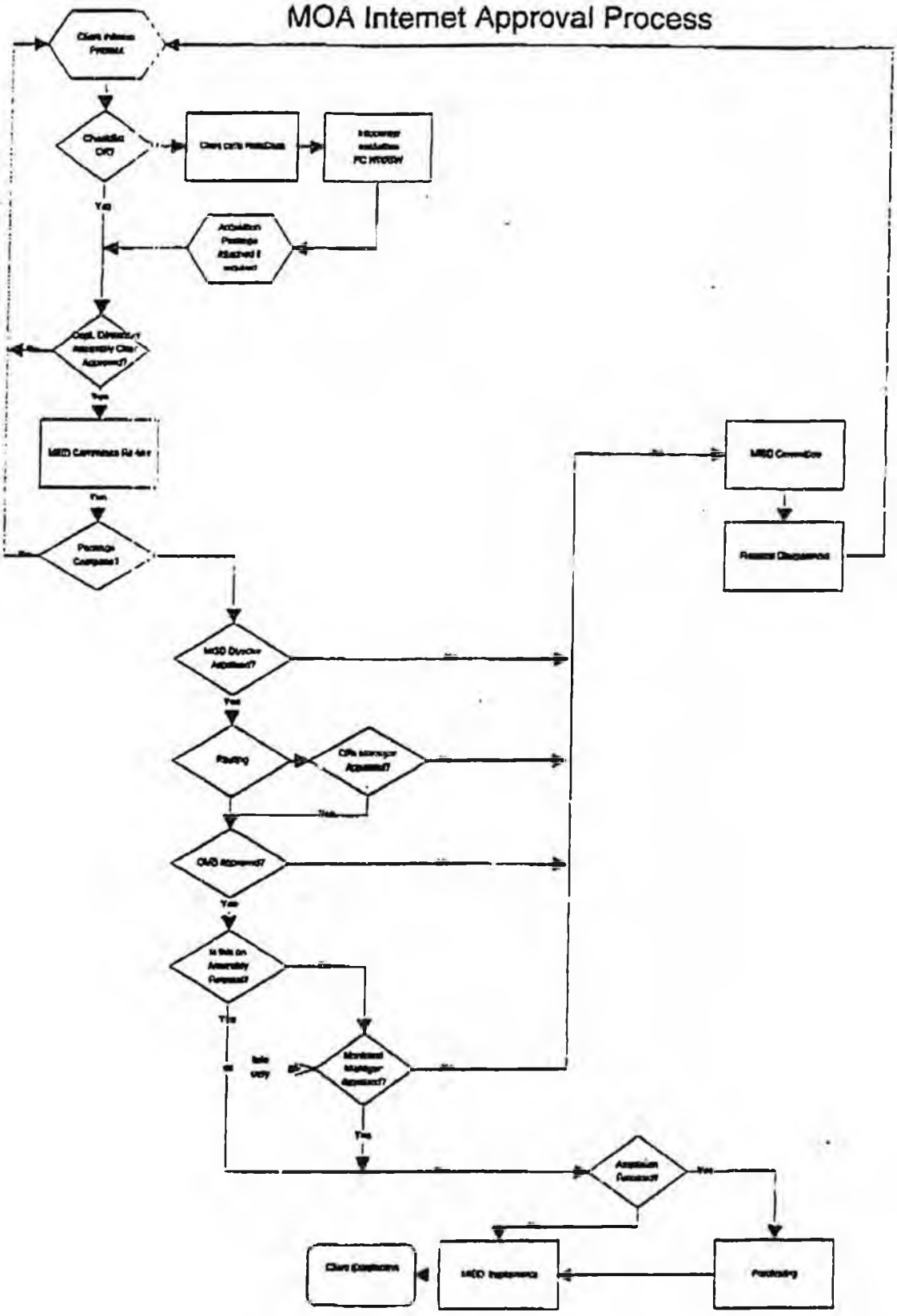
Requesting Employee's Printed Name **Requesting Employee's Signature** **Date**

_____ _____

Employee Department / Division **Employee Phone #**

APPROVAL ROUTING

			Packet Complete
1) Department Director or Assembly Chair	**Date**	2) MISD Committee Review	☐ Yes ☐ No
3) MISD Director	**Date**	4) Operations Manager Approval (If Required)	**Date**
5) OMB Approval	**Date**	6) Municipal Manager or Designee Approval	**Date**



ATTACHMENT B

ALASKA STATE LEGISLATURE
House of Representatives

COMMITTEE ASSIGNMENTS:

LABOR & COMMERCE COMMITTEE, CHAIRMAN
SPECIAL COMMITTEE ON OIL & GAS, MEMBER
JUDICIARY COMMITTEE, MEMBER
CORRECTIONS BUDGET SUBCOMMITTEE, MEMBER
ADMINISTRATION BUDGET SUBCOMMITTEE ,MEMBER
HESS BUDGET SUBCOMMITTEE, MEMBER

INTERIM:
716 WEST 4TH AVENUE, SUITE 640
ANCHORAGE, AK 99501
PHONE: (907) 258-8191
FAX: (907) 258-2916

SESSION:
STATE CAPITOL
JUNEAU, AK 99801-1182
PHONE: (907) 465-4968
FAX: (907) 465-2040

Representative Norman Rokeberg

MEMORANDUM

TO: House Labor & Commerce Committee Members

FROM: Representative Norman Rokeberg

DATE: March 27, 1998

RE: HB 319

During the committee meeting on the captioned bill, questions were asked about legislative policy. For your information:

1. Confidentiality of Information on Desktop Computers. In accordance with the Public Records Policy regarding Legislators' records adopted by the Legislative Council on March 14, 1997, the Agency shall treat all documents, files and data on Legislators' desktop computer systems as confidential information. (Source: Legislative Council, Policy on Desktop Computer Support, Software and Hardware, Amended April 29, 1997, page 3.)
2. Personally Owned Desktop Computers. The Agency shall support personally owned desktop computer systems until such time as they are replaced with standard systems. The Agency shall review each personally owned desktop computer before connecting it to the network and may restrict the connection if the system is determined to be incompatible with the network. Support for standard desktop computer software and hardware shall take precedence over personally owned systems. (Source: Legislative Council, Policy on Desktop Computer Support, Software and Hardware, Amended April 29, 1997, page 6.)
3. Legislator's Records. The Legislative Council finds that records of a legislator while in the possession of that legislator are not public records based on the deliberative process privilege and on Art. II, sec. 6, Alaska Constitution. Therefore a legislator's records are not subject to disclosure under AS 09.25.110-09.25.122. Each legislator may, at his or her discretion, elect to release or not to

> release information from that legislator's own records. However, the Council recognizes that public information that is available from another agency or governmental entity may be obtained by any person directly from that agency even if a legislator declines to make the same information available from the legislator's own records. (Source: Records Policy which accompanied a December 24, 1997 memorandum from Pamela Varni, p. 1)

If you would like complete copies of the referenced policies, please contact Pamela Varni, Executive Director, Legislative Affairs Agency, 465-3800.