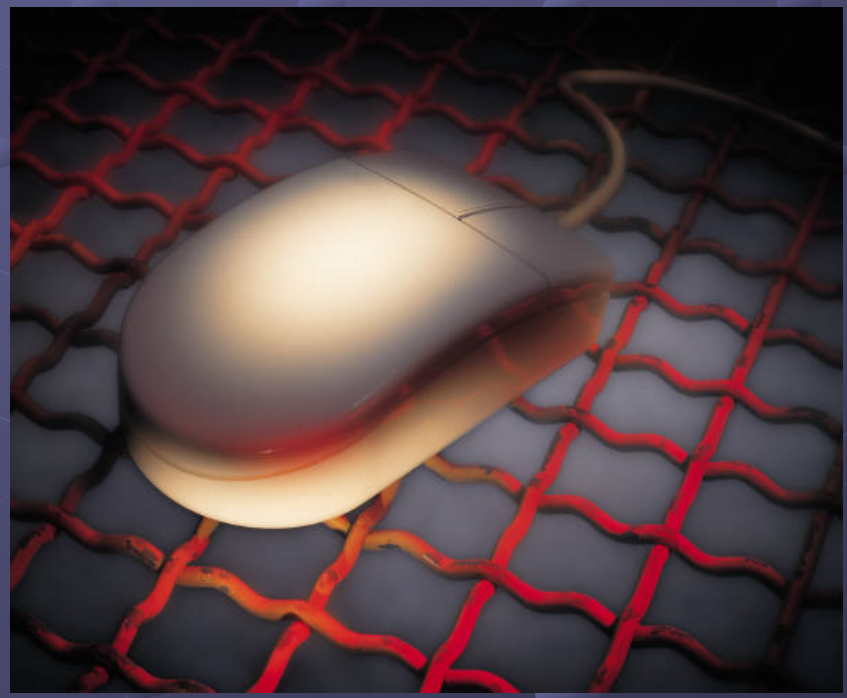
ACCOUNTABILITY FOR COMPUTER AND INTERNET MISUSE



OBJECTIVES

- Address guidelines for computer use
- Discuss detection of computer misuse, evidence collection and evaluation.
- Address elements of proof and charge formulation

OBJECTIVES

- Discuss affirmative defenses and computer misuse as a disability
- Discuss charges that have been successfully used in adverse actions
- Discuss preventive measures

GUIDELINES FOR COMPUTER USE

- The First Amendment
- The Fourth Amendment
- Electronic Communications Act
- Agency Computer Use Policy

THE FOURTH AMENDMENT

- The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

THE FOURTH AMENDMENT

- A warrantless search is permissible if it does not violate an individual's "reasonable" expectation of privacy
  - An actual expectation
  - Society recognizes expectation as reasonable
- Search violates an expectation of privacy, but is nonetheless reasonable

THE FOURTH AMENDMENT

- Computer searches
  - Regarded as “closed containers”
  - Expectation of privacy not retained if:
    - Computer is made openly available
    - Control is relinquished to a third party
    - Data is communicated over networks (email) once it reaches intended recipient
  - Does not apply to searches conducted by private parties

THE WORKPLACE

- Public sector employees
  - Reasonable expectation of privacy only so far as the office practice, procedures or regulations permit the employee's supervisor, coworkers or the public to enter the employee's workspace
  - Employers can conduct "reasonable" searches, even if it violates the expectation of privacy

THE WORKPLACE

- Searches must be
  - Work related
  - Justified at their inception
  - Permissible in scope

ELECTRONIC COMMUNICATIONS PRIVACY ACT

The Electronic Communications Privacy Act (ECPA) sets out the provisions for access, use, disclosure, interception and privacy protections of electronic communications. Enacted in 1986, the law covers various forms of wire and electronic communications. According to the U.S. Code, electronic communications "means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce."

ELECTRONIC COMMUNICATIONS PRIVACY ACT

- Banners
  - A posted notice informing users as they log on to a network that their use may be monitored, and that subsequent use of the system will constitute consent to the monitoring. Every user who sees the banner before logging on to the network has received notice of the monitoring: by using the network in light of the notice, the user impliedly consents to monitoring pursuant to 18 U.S.C. § 2511(2)(c)-(d)

ELECTRONIC COMMUNICATIONS PRIVACY ACT

- Banner notices should consider:
  - the network's purpose
  - the system administrator's needs
  - the users' culture

AGENCY POLICY

- Scope
  - To whom will the policy apply?
  - To what extent may employees access electronic equipment for personal use?

AGENCY POLICY

- Elements
  - Employee privileges and responsibilities
  - Definitions
  - Provisions for use of equipment and services
  - Proper representation

AGENCY POLICY

- Elements (cont.)
  - Privacy expectations and consent to monitoring
  - Sanctions for misuse should include specific examples of what constitutes inappropriate use

COLLECTION OF EVIDENCE

- REPORTING SOURCES
  - Supervisor
  - Coworker
  - Member of the public
  - Information technology/systems security personnel
  - Anonymous source

COLLECTION OF EVIDENCE

- Who is responsible?
- What type of investigation will be conducted?
  - Administrative
  - Criminal

COLLECTION OF EVIDENCE

- Directives and regulations
- Policies
- Banners
- Invoices
- Computer training courses

COLLECTION OF EVIDENCE

- Layout of the office area
- Physical location of the computer
- Is the computer password protected?
- Who has access to the computer?
- Are information systems security practices followed?

COLLECTION OF EVIDENCE

- How many computers are assigned to the employee?
- How many email accounts does the employee have?
- What are the employee's official duties?
- Does the employee handle sensitive information?
- What is the employee's knowledge of computers?

COLLECTION OF EVIDENCE

- Operating systems
- Network or stand alone?
- Desktop or laptop?
- Software or hardware?
- Peripherals?
- Network services?

STATE OF OHIO vs. BRIAN N. COOK

- The Court of Appeals of Ohio held that "mirror image" of hard disk from defendant's computer was properly authenticated for admission
  - Software is commercially available to recover files/images that have been deleted and/or overwritten
  - Supports use of sophisticated evidence collection techniques; used “Encase” software

EVALUATE THE EVIDENCE

- What kind of evidence do you have?
- What does the evidence prove?
- Where are the holes?
- What is the employee's explanation?

ELEMENTS OF PROOF

- Must establish/prove information was downloaded by employee in question
  - May require access to employee's T&A
  - May require access to employee's Internet account
- Important to know when image was downloaded/sent
  - "Internal clock" inside computer needs to be turned "on"

ROADBLOCKS TO SUCCESSFUL CASE DEVELOPMENT

- Dealing with highly unstable media
- Employee may run “window washing” programs to “overwrite” disk
- Computer may have been in the possession of more than one user
- Employee may be using another computer (other than his/her own) to engage in the misconduct

FRAMING CHARGES

- Evaluate the evidence you have
- Develop alternative charges
- Look at current, relevant case law
- Refine the charges, in clear language that distinguishes charges from specifications

DEVELOP ALTERNATIVE CHARGES

- Stick to plain language
- Avoid terms with specific meanings in criminal law
- Consider charges that cite agency policy (give examples)

REFINE THE CHARGES

- Use clear language to distinguish charges from specifications
- Tell employee clearly what charge is going to be proved
- Avoid terms associated with specific burdens of proof (e.g., pornography)

DEFENSES

- Computer misuse as an addiction
- Reasonable accommodation as an affirmative defense

DEFINITION OF DISABILITY

- Under the ADA, an individual with a disability is a person who has:
  - a physical or mental impairment that substantially limits one or more major life activities;
  - a record of such a impairment; or
  - is regarded as having such an impairment

29 CFR 1630.3

- *Disability does not include:*

  Transvestism, transsexualism, pedophilia, exhibitionism, voyeurism, gender identity disorders not resulting from physical impairments, or other sexual behavior disorders

  - *William C. White vs. Dept. of Army* CH-0752-00-05450-I-1, July 20, 2000
  - *Cambron vs. Postal Service* SF-0752-99-0100-I-1, 5/27/99

THE VIEW FROM THE MSPB AND THE COURTS

THE SUPREME COURT DEFINES PORNOGRAPHY

- *Roth vs. US*, 354 US 476 (1957)
  - "The test in each case is the effect of the book, picture or publication considered as a whole not upon any particular class, but upon all those whom it is likely to reach. In other words, you determine its impact upon the average person in the community… You may ask yourselves does it offend the common conscience of the community by present day standards."

THE SUPREME COURT DEFINES PORNOGRAPHY

- *Jacobellis vs. State of Ohio* 378 US 184 (1964)
  - "The test for obscenity is whether to the average person, applying contemporary community standards, the dominant theme of the material, taken as a whole, appeals to prurient interest."
  - Justice Stewart, in concurring opinion, "I know it [pornography] when I see it"

CHARGES SUSTAINED IN AGENCY ADVERSE ACTIONS

- Misuse of Government Resources (*Cobb vs. Air Force*, 57 MSPR 47)
- Using the Agency's Electronic Mail System to Write Love Notes (*Dolezal vs. Army*, 58 MSPR 64)
- Misuse of Government Computer (*Morrison vs. NASA*, 65 MSPR 348)

CHARGES SUSTAINED IN AGENCY ADVERSE ACTIONS

- Improper Use of Government Equipment; Deliberate Misrepresentation of Facts Pertaining to Use of Email/Internet (*Rush vs. Air Force,* 69 MSPR 416)
- Using Government Resources to Work on Private Business (*Avant & Kratz vs. Air Force,* 71 MSPR 192)
- Misuse of Official Time and Government Property (*Cox vs. Interior,* DA-0752-97-0376-I-1, 9/25/97)

CHARGES SUSTAINED IN AGENCY ADVERSE ACTIONS

- Unauthorized Access of Employees' Email Accounts; Unauthorized Disclosure of Information; Providing False Information to Supervisor in Connection with a Factfinding; Unauthorized Use of an Agency Computer System to View and Forward Sexually Explicit Material to Another Agency Employee and to Other Persons Outside of the Agency; Unauthorized Monitoring of his Supervisor's VISTA Access

(*Michael L. Schoeny vs. Dept. of Veterans Affairs,* CH-0752-02-0682-I-1, July 23, 2003)

CHARGES SUSTAINED IN AGENCY ADVERSE ACTIONS

- Unauthorized Disclosures; Conduct Unbecoming a DEA Special Agent; Misuse of Office; Misuse of Government Property (*Regina Bledsoe vs.. Dept. of Justice,* 91 MSPR 93, March 11, 2002

- Misuse of Government Computer; Wasting Time (*Kirk J. McDaniel vs. Dept. of Navy,* CH-0752-03-0779-I-1, December 4, 2003

- *Cambron vs. Postal Service* SF-0752-99-0100-I-1, 5/27/99

LABOR RELATIONS

- Impact and implementation bargaining of agency policy
  - Many elements include components of system security and may be non-negotiable
  - Proposals for banner language that distort the intent of the notice may be non-negotiable
  - *AFGE vs. SSA, HQ, Baltimore*, 103 FLRR 2-1063

LABOR RELATIONS

- Weingarten meetings
  - Bargaining unit employees are entitled to union representation during investigatory interviews
  - The employee must request representation

AN OUNCE OF PREVENTION…

- Supervisor/Management awareness training that it is a problem
  - Loss of productivity
  - Security breaches
  - Loss of bandwidth=$$
- Improve relationship with IT
  - Set out expectations for evidence
  - “Hog” reports

AN OUNCE OF PREVENTION…

- Employee Relations/IT/OIG Collaboration
  - How will investigations be conducted
  - What must we ask to get what we need
  - Confidentiality
  - Bargaining unit status of IT/ISSOs
  - Equitable disclosure of information
  - Work together on banner language

AN OUNCE OF PREVENTION…

- Consider having IT monitor previous “misusers”
- Detection software
- Firewalls

REFERENCES

- http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm
  "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, July 2002.
- http://www.cyberfeds.com
  Recommended Executive Branch Model Policy/Guidance on "Limited Personal Use" of Government Office Equipment including Information Technology

THE PRESENTERS

Leslie Violette, Chief, Employee/Labor Relations & Benefits Branch, US Dept of Agriculture, (202)720-8351, leslie.violette@usda.gov

Latonia Parham, Employee & Labor Relations Specialist, US Dept of Health & Human Services, (301)827-4191, lparham@psc.gov