Email Access: Privacy Issues Regarding Use of County Email Systems

W. Lewis Black

Dunn & Dunn, P.C.


He got an e-mail that was actually work related...
the shock was too much...

Agenda

- 1. State Laws and Policies
- 2. Recent Cases
- 3. Policy Examples
- 4. Best Practices

State Laws and Policies

Government Records Access and Management Act (GRAMA) – U.C.A. § 63G-2-103(22)(a)

- A “Record” is:
  - A book, letter, document, paper, map, plan, photograph, film, card, tape, recording, electronic data, or other documentary material, regardless of physical form or characteristics, that is prepared, owned, received, or retained by a government entity or political subdivision where all the information in the original is reproducible by photocopy or other mechanical or electronic means.
- If an email is sent or received as part of a State business transaction, be it an interagency transaction or business with an entity outside of State government, it is considered a record.
  - Email that is work-related and has administrative, legal, fiscal, or historical value, is a record.
  - Drafts, personal notes or communications, proprietary software, copyrighted material, junk mail, commercial publications, and personal daily calendars are not records.

Internet Employment Privacy Act – U.C.A. §§ 34-48-101 to -301

- An Employer cannot:
  - Request that an employee or applicant disclose a password, or a username and password, that would allow the employer access to the employee's or applicant's ***personal*** internet account; or
  - Take adverse action, fail to hire, or otherwise penalize an employee or applicant for not disclosing the above information.

Internet Employment Privacy Act – U.C.A. §§ 34-48-101 to -301 (Continued)

- An Employer may:
  - Request of require an employee to disclose a username or password to gain access to:
    - An electronic communications device that the employer supplies or pays for in whole or in part; or
    - An account or service that the employee obtained by virtue of the employee's employment relationship and used for the employer's business purposes.
  - Discipline or discharge an employee for transferring any of the following to an employee's personal internet account without the employer's authorization:
    - Proprietary or confidential information; or
    - Financial data.

Internet Employment Privacy Act – U.C.A. §§ 34-48-101 to -301 (Continued)

- An Employer May:
  - Investigate if:
    - There is specific information on the employee's personal internet account, to ensure compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct; and
    - The employer has specific information about an unauthorized transfer of the employer's proprietary information, confidential information, or financial data to an employee's internet account.
  - Restrict or prohibit an employee's access to certain websites while using:
    - An electronic communications device supplied or paid for (in whole or in part) by the employer; or
    - An employer's network or resources.

Internet Employment Privacy Act – U.C.A. §§ 34-48-101 to -301 (Continued)

- An Employer may:
  - View, access, or use information about an employee or applicant that:
    - Can be obtained without the employee's username or password to a personal account; or
    - Is available in the public domain.

Internet Employment Privacy Act – U.C.A. §§ 34-48-101 to -301 (Continued)

- The act does not specifically address email communications.
- If found in violation of the Act, an employer may be required to pay the aggrieved individual up to $500 in damages.

Utah Interception of Communications Act – U.C.A. §§ 77-23A-1 to 77-23A-16 and 7-24B-1 to 7-24B-9

- A person may intercept wire, electronic, or oral communication only if either:
  - The person is a party to the communication; or
  - One of the parties to the communication has given prior consent to the interception.
- A person cannot obtain, alter, or prevent authorized access to a wire or electronic communication while it is in an electronic storage system if the person intentionally either:
  - Accesses without authorization a facility through which an electronic communications service is provided; or
  - Exceeds an authorization to access the facility.

Utah Interception of Communications Act – U.C.A. §§ 77-23A-1 to 77-23A-16 and 7-24B-1 to 7-24B-9 (Continued)

- A person or entity may divulge the contents of a communication:
  - To an addressee or intended recipient of the communication or an agent of the addressee or intended recipient;
  - With the consent of either:
    - The originator;
    - The addressee; or
    - The communication's intended recipient.
  - To a person employed or authorized, or whose facilities are used to forward the communication to its destination;
  - As may be necessarily incident to the rendition of the service or the protection of the rights or property of the provider of that service; or
  - To a law enforcement agency in certain situations.
- If the employer is found liable, the aggrieved individual may obtain:
  - Preliminary and other equitable or declaratory relief as appropriate;
  - Compensatory and punitive damages in appropriate cases; and
  - Reasonable attorneys' fees and court costs.

Utah Protection of Public Employees Act (Whistleblower Act) – U.C.A. §§ 67-24-1 to 67-24-10

- A public employer cannot take an adverse action against a public employee because the employee communicates in good faith:
  - The waste or misuse of public funds, property, or manpower;
  - A violation or suspected violation of a law, rule, or regulation adopted under the law of this state, a political subdivision of the state, or any recognized entity of the United States; or
  - As it relates to a state government employer:
    - Gross mismanagement; or
    - Abuse of authority, or unethical conduct.

Electronic Mail for State Agencies: A Guideline of the Utah State Archives and Records Service (March 2017)

- Essential Elements of an Email Management System
  - Each State agency should require that it use an approved electronic records management system or develop a policy of their own that complies with the baseline standards of said system.
  - A management system includes:
    - Hardware;
    - Software;
    - Storage system used to manage email; and
    - A policy that describes how the system is used and the records it contains.
  - The policy must require that all State business is conducted on computers and devices that are connected to an authorized management system.

Electronic Mail for State Agencies: A Guideline of the Utah State Archives and Records Service (March 2017) (Continued)

- Retention and Disposition of Correspondence
  - Retention schedules are created to account for any administrative, fiscal, legal, or historical value that may be contained in a record so that it may be disposed of appropriately.

Electronic Mail for State Agencies: A Guideline of the Utah State Archives and Records Service (March 2017) (Continued)

- General Retention Schedules currently used:
  - Transitory Correspondence
    - Incoming and outgoing correspondence, regardless of format or mode of transmission, related to matters of short term interest.
    - Contains no final contractual, financial, or policy information.
    - Does not impact agency functions.
    - Retention:
      - Retain until administrative need ends and then destroy.
      - See Utah State General Records Retention Schedule, Transitory Correspondence (Item 4-11).

Electronic Mail for State Agencies: A Guideline of the Utah State Archives and Records Service (March 2017) (Continued)

- General Retention Schedules currently used (Continued):
  - Administrative Correspondence
    - Incoming and outgoing correspondence, regardless of format or mode of transmission, created while administering agency functions and programs.
    - Documents work accomplished, transactions made, or actions taken.
    - Documents the implementation of agency functions rather than the creation of functions or policies.
    - Retention:
      - Retain for 7 years and then destroy
      - See Utah State General Records Retention Schedule, Transitory Correspondence (Item 4-12).

Electronic Mail for State Agencies: A Guideline of the Utah State Archives and Records Service (March 2017) (Continued)

- General Retention Schedules currently used:
  - Executive Correspondence
    - Incoming and outgoing correspondence, regardless of format or mode of transmission, that provides unique information relating to the functions, policies, procedures, or programs of the agency.
    - Documents executive decisions made regarding agency interests.
    - Retention:
      - Permanent. May be transferred to the State Archives.
      - See Utah State General Records Retention Schedule, Transitory Correspondence (Item 4-10).

Cases (Private Employers)

Walston v. United Parcel Service, 2008 WL 5191710 (D. Utah 2008)(unpublished)

- An employee has a reasonable expectation of privacy when the privacy invasion would be "offensive to a reasonable person." 2008 WL 5191710 at *3.

U.S. v. Warshak, 631 F.3d 266 (6th Cir. 2010)

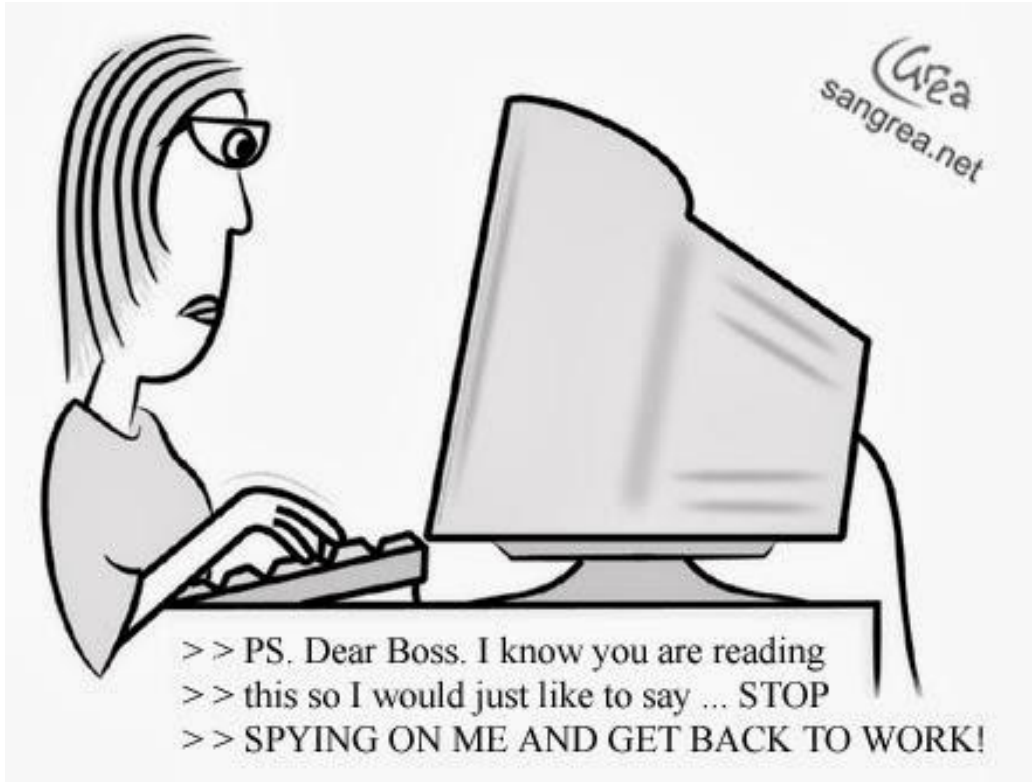
- Defendants were found guilty of conspiracy to commit bank fraud, bank fraud, and money laundering. Defendants argued on appeal that government agents violated their Fourth Amendment Rights by seizing 27,000 private emails without a warrant.
- The Sixth Circuit Court held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a ***commercial*** ISP." 631 F.3d at 288 (Emphasis added).

U.S. v. Young, 2013 WL 6665378 (D. Utah 2013)(unpublished)

- Defendant filed a Motion to Suppress challenging warrants and the subsequent searches and seizures of computers from his office and his attorneys' offices, and emails from his personal and business accounts.
- Judge Campbell held that a "sender of email loses his or her reasonable expectation of privacy in an e-mail that has actually reached the intended recipient." 2013 WL 6665378 at *2.

Cases stating that there is no reasonable expectation of privacy in using an employer's email system

- *Bingham v. Baycare Health System*, 2016 WL 3917513 (M.D. Fla. 2016)(unpublished)
- *Billings Gazette v. City of Billings*, 313 P.3d 129 (Mont. 2013)
- *U.S. v. Hamilton*, 2011 WL 1366481 (E.D. Pa. 2011)(unpublished)
- *U.S. v. Monroe*, 52 M.J. 326 (C.A.A.F. 2000)
- *McLaren v. Microsoft Corp.*, 1999 WL 339015 (Tex. App. 1999)(unpublished)
- *Smyth v. Pillsbury Co.*, 914 F.Supp. 97 (E.D. Pa. 1996)



Public Employers

City of Ontario, Cal. v. Quon, 560 U.S. 746, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010)

- City police officer brought a § 1983 action against city, police department, and police chief, alleging that the police department's review of officer's text messages violated his Fourth Amendment Rights. Officer claimed that he had a reasonable expectation of privacy in his text messages, based on actions of his superior.
- The U.S. Supreme Court held that the search was reasonable on Fourth Amendment grounds, but did not address the expectation of privacy issue.
- "The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." 560 U.S. at 759.

Sollenberger v. Sollenberger, 173 F.Supp. 3d 608 (S.D. Ohio 2016)

- Former sheriff's office detective brought suit against, among others, his estranged wife and the sheriff, alleging violations of the Fourth Amendment and various state law torts including invasion of privacy regarding information extracted from an old cell phone left at his wife's house when he moved out. The information extracted from the cell phone corroborated other evidence of the plaintiff's work-related misconduct.
- The court, citing *Quon*, held that the plaintiff's expectation of privacy was not a clearly established constitutional right.
- The court also found that the search of the old cell phone was reasonable in scope.

City of San Jose v. Superior Court, 389 P.3d 848 (Ca. 2017) (March 2, 2017)

- Resident of city brought action against city, mayor, and ten city council members for declaratory judgment that the California Public Records Act required disclosure of their private voicemails, e-mails, and text messages relating to city business.
- The California Supreme Court held that when a city employee uses a personal account to communicate about the conduct of public business, the writings may be subject to disclosure under the Act.
- "The issue is a narrow one: Are writings concerning the conduct of public business beyond CPRA's reach merely because they were sent or received using a nongovernmental account? Considering the statute's language and the important policy interests it serves, the answer is no. Employees' communications about official agency business may be subject to CPRA regardless of the type of account used in their preparation or transmission." 389 P.3d at 852.

U.S. v. Cochran, 2017 WL 1032573 (11th Cir. 2017)(unpublished) (March 17, 2017)

- Former county chief magistrate judge was convicted of several felonies and was sentenced to 60 months in prison. Among the charges against him was the violation of a court secretary's constitutional rights by searching her cell phone without permission on at least two occasions. The defendant appealed his convictions, arguing, among other things, that he did not have fair warning at the time of the offense that searching an employee's cell phone without permission was a constitutional violation.
- The 11th Circuit Court vacated the defendant's conviction on this count, holding that they were unable to conclude that he had the required "fair warning" that his actions were in violation of a clearly established constitutional right.
- "[W]hen conducted for a noninvestigatory, work-related purpose or for the investigation of work-related misconduct, a government employer's warrantless search is reasonable if it is justified at its inception and if the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the circumstances giving rise to the search." 2017 WL 1032573 at *10.

Examples of Email Policies

Expectation of Privacy

- “No County employee should have any expectation of privacy as to his or her Internet usage.”
- “All data, facsimiles, e-mail, and voice mail are the property of the County, and users shall not have an expectation of privacy in this regard. Users should not assume electronic communications are totally private and confidential and should transmit private and sensitive information in other ways.”
- “All electronic data is the property of the County and electronic records are County records. Therefore, employees have no right or expectation of privacy in internet, e-mail, or other electronic records resources provided by the County. Employees should be aware that the County has the right to inspect all electronic files, records, and resources, including e-mail messages and internet activity logs. The Human Resources Department may authorize access to any employee’s electronic records resources at any time and without notice.”

Personal Phone Use

- “When employees receive an allowance or reimbursement for business use of their personal cell phone, their personal information will generally not be subject to GRAMA or will be considered “private” under GRAMA. However, because personal data is comingled with business data, an employee’s personal data is subject to inspection by the County or court in response to a GRAMA request, discovery or court action related to the business data. Business data is subject to the County retention schedule and may be subject to litigation standards.”
- “Employees are responsible for maintaining a copy of their personal cell phone bills for at least one year for auditing purposes.”
- “Long distance dialing of County-owned telephones for personal business is strongly discouraged and shall be allowed only in emergency situations.”

Personal Use of County Equipment

- “Electronic communication devices and services shall not be used for knowingly transmitting, receiving, retrieving, or storing any communications which are derogatory to any individual group, are pornographic, lewd, indecent, or of a sexual nature, or are of a defamatory or threatening nature.”
- “Electronic communication devices and services shall not be used in a manner which could be construed as discriminatory based on race, national origin, sex, age, disability, genetic information, or religious or political beliefs.”
- “Electronic communication devices or services shall not be used for communication of chain letters, or for any purpose which is illegal, against County policy, or contrary to the County’s interests.”

Personal Use of County Equipment (Continued)

- "Employees must use electronic communication devices and services primarily to accomplish their specific job descriptions. However, employees may use electronic communication devices and services incidentally for personal purposes so long as the use complies with the following restrictions:
  - During regular work hours, the use should be short and infrequent and must NEVER interfere with an employee's work; and personal use should preferably occur during the employee's personal time;
  - The use should enhance job performance, such as educating the employee or improving job-related skills;
  - The County must not incur more than insignificant cost as a result of the use;
  - The use must not overburden the communications system;
  - The use must not involve any activity that reflects adversely on the County or is incompatible with public service; and
  - This use must adhere to all other requirements of this policy."

Personal Use of County Equipment (Continued)

- Examples of Permitted Use (Unless Your Department Head Has Stricter Standards):
  - “Emailing short messages to relatives, friends, or associates;
  - Scheduling medical appointments, arranging for home or auto repairs, making travel arrangements, or other appointments;
  - Brief internet searches of sites that would not reflect adversely on the County;
  - Receiving and sending email comparable to acceptable non-disruptive telephone messages;
  - Making a bank transaction.”

Personal Use of County Equipment (Continued)

- "The following are prohibited:
  - Attempting to obtain authentication information without authorization or breaking into any electronic communication resource;
  - Seeking or obtaining unauthorized access to another employee's electronic communication resource;
  - Sending a threatening message or making personal attacks on others that could be construed as defamation;
  - Accessing, viewing, downloading, or transmitting sexually oriented material;
  - Transmitting derogatory material that may be construed as harassment based on race, color, national origin, sex, age, disability, or religion;
  - Gambling;
  - Office gossip;
  - Violation of any law or regulation;
  - Theft or copying of electronic files without permission or disobeying any copyright law;
  - Sending or posting County confidential or proprietary material to any unauthorized recipient;
  - Sending electronic chain letters, Spam, or unsolicited junk mail through email;
  - Sending or soliciting messages that could damage the image of the County;
  - Loading onto the system counterfeit, unauthorized, or copies of software that are not licensed to the County;
  - Attempting to circumvent any system intended to protect the privacy or security of IT;
  - Refusing to cooperate with an IT investigation;
  - Using the County's name in an official way in electronic communications when not explicitly authorized to do so."

Monitoring Procedures

- “The Information Technology Department shall audit the use of laptop computers twice per year to ensure compliance with this policy. Users shall be responsible for any charges arising from personal use of equipment, computers, laptop computers, electronic communication devices or services. Users are expected to act responsibly and shall be subject to disciplinary action if this privilege is abused.”
- “The County routinely monitors usage patterns for both voice and data communications for cost analysis and Internet management (e.g., number called or site accessed, call length, call frequency, etc.).”
- “The County has software and systems in place that can monitor and record all internet usage.”
- “The County reserves the right, at its discretion, to review any user’s electronic files/messages and usage to the extent necessary to ensure that electronic communication devices and services are being used in compliance with the law and County policy and may disclose the contents of any user’s electronic files/messages and usage of electronic media and services for a business or legal purpose.”

County Property

- “Electronic communication devices and services provided by the County are County property, their purpose is to facilitate County business, and their use is subject to County control and policy.”
- “This policy applies to all electronic communication devices and services which are accessed on or from County premises, are accessed from remote locations using County computer equipment or via County paid access methods, and/or are used in a manner which associates the individual with the County.”

Miscellaneous Provisions

- “Any message or information sent via an electronic network (i.e., bulletin board, on-line service, or Internet) are statements identifiable and attributable to the County. Use of personal disclaimers in an electronic communication will not relieve any user under this policy and users shall be held responsible for any communication initiated by them.”
- “No email or other electronic communications shall be sent which attempts to hide the identity of the sender or misrepresent the sender.”
- “Users shall not reveal their passwords without a business necessity or otherwise breach the security of the County’s electronic communication system.”
- “Anyone obtaining electronic access to other organizations’ or individuals’ materials must respect all applicable laws and shall not copy, retrieve, modify, or forward copyrighted materials except as expressly permitted by the copyright owner.”

Best Practices/Recommendations

- If possible, have a ***CONSISTENT*** County-wide policy.
- ***INFORM*** employees ***IN WRITING*** that there is no expectation of privacy in public business or in government-provided electronic communications devices.
- ***EDUCATE*** your employees about all aspects of the policy (and have periodic refresher courses).
- ***IMPLEMENT*** and ***ENFORCE*** all policies consistently.
- ***AVOID*** using personal email to conduct official business.
- ***REMEMBER:*** Public business conducted on private email accounts is still a public record.
- ***DON'T*** mix personal and professional topics in the same email.
- ***WHEN IN DOUBT***, err on the side of caution.
- Don't be afraid to ***ASK FOR HELP***; you will probably need it sooner than you think.

"I found a solution to your spam problem. I've set up your e-mail to automatically delete any message with a vowel in it."

THANK YOU!

DUNN & DUNN
ATTORNEYS AT LAW

Susan Black Dunn
sblack@dunndunn.com
W. Lewis Black
wlblack@dunndunn.com

2455 East Parley's Way
Suite 340
Salt Lake City, Utah 84109
(801) 521-6677