June 2014

The Local Government Liability Beat

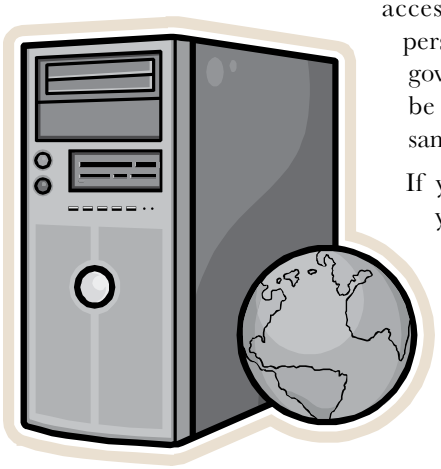
PRESENTED BY LOCAL GOVERNMENT RISK MANAGEMENT SERVICES INC · A SERVICE ORGANIZATION OF
THE ASSOCIATION COUNTY COMMISSIONERS OF GEORGIA AND THE GEORGIA MUNICIPAL ASSOCIATION RISK MANAGEMENT PROGRAMS

Internet, Email, and Electronic Communication

By Dennis Watts

In this Liability Beat, we are providing an Internet Use and Online Social Networking Policy for Law Enforcement and Internet and Electronic Communication Sample Policies for general use. Both can be modified to suit your needs. We are also including an article that is a bit of a twist on Fourth Amendment seizures normally associated with law enforcement. In this case, the Sixth Circuit Court in *United States v. Overton* is about firefighters.

Social media in general continues to be an area of concern, particularly with Title VII Harassment issues. LGRMS provides harassment training, both on a regional basis and onsite, at no cost to your entities which cover these issues. Many of you already have policies covering the use of electronic media; some of you do not. This is an area that has gained increased attention over the last several years. Many of our elected officials and employees are unaware of the potential issues in using email and how inappropriate use could compromise personnel actions or create or affect liability concerns. Electronic media, particularly email, has drastically changed how both individuals and businesses communicate. This has made possible many positive communication and coordination benefits in our daily activities as we do business for our citizens. On the downside, it has created additional liability exposures that most individuals are not aware of.



Sending jokes, innuendos, or other off-color content to recipients might seem like innocent fun until a defense attorney uses it in court. Pressing the delete button does not really get rid of the document; it is still out there and accessible. We tend to think of our emails as personal and private, but in the world of local government (and private business, too), it can be very public, as stated in section 4 of the sample policy.

If you currently have a policy, we encourage you to review it, compare it to our sample policy, and update if needed. If you do not currently have a policy, review our sample and consider adopting it or creating your own version. Have your city or county attorney review it, and then make sure all affected employees and elected officials understand the intent of the policy.

Detention by Firefighters for Medical Treatment Held a Seizure under the Fourth Amendment

By Brian S. Batterton, Attorney, PATC Legal & Liability Risk Management Institute

When law enforcement officers restrict a person's freedom of movement, the officer has seized that person under the Fourth Amendment. At times, firefighters will also restrict a person's movement, sometimes against that person's will, for the purpose of providing medical treatment or an evaluation. On April 15, 2014, the Sixth Circuit Court of Appeals decided *the United States v. Overton,*[i] which illustrates how seizure by fire personnel also implicates the Fourth Amendment.

In Overton, on or about April 29, 2012, Bennie Overton committed a carjacking, stealing Gore's car. Then:

Five days later, on May 4, 2012, Cincinnati Fire Department personnel ("EMS personnel") received a 911 call for emergency medical assistance, relating to a "reported

unconscious person in a vehicle at the gas pumps" of a gas station on Gilbert Avenue. Upon arriving at the gas station, the EMS personnel saw their patient (later identified as Overton) leaning back in the driver's seat of a silver sedan (later identified as Gore's 2004 Nissan Maxima). The patient was "in the driver's seat, eyes closed, unresponsive, the doors closed." After blowing the fire truck's air horn and administering ammonia inhalants in unsuccessful attempts to rouse Overton, the EMS personnel employed a sternum rub technique to wake him.

Upon waking, Overton seemed confused and disoriented and grabbed the shirt of the firefighter who administered the sternum rub. While the EMS personnel were talking to Overton and attempting to ascertain his condition, he shifted his legs in his seat and exposed the handle of a .45 caliber pistol. At this point, the EMS personnel began to get nervous for their safety and the safety of those around them. They accordingly removed Overton from the car and secured the pistol.

On June 6, 2012, a grand jury indicted Overton for the following crimes: one count of carjacking, one count of using, carrying, or brandishing a firearm in furtherance of a crime of violence, and one count of being a felon in possession of a firearm. Overton filed a motion to suppress the pistol discovered by the EMS personnel, which the district court denied after an evidentiary hearing. Overton then pled guilty to the felon in possession of a firearm count on August 13, 2012, but proceeded to a jury trial on the carjacking and brandishing offenses. The trial took place over three days in August of 2012, and the jury returned guilty verdicts on both remaining counts. The district court then sentenced Overton to a within-Guidelines term of 199 months' imprisonment, five years of supervised release, a $1,000 fine, and the forfeiture of various items. Overton filed a Notice of Appeal the day after the district court entered judgment, and this appeal followed. [ii]

Overton raised numerous issues on appeal, one of which that the gun should have been suppressed because it was the fruit of an illegal seizure of his person by firefighters when they detained him for about 30 seconds after they awoke him using the sternum rub. The firefighters testified that they would not have let Overton leave immediately after wakening him because they feared his health was in jeopardy.

The court of appeals first stated:

> As the Supreme Court repeatedly has held, a person is seized for Fourth Amendment purposes when a reasonable person in his circumstances would not feel free to leave. E.g., *Michigan v. Chesternut*, 486 U.S. 567, 573 (1988) ("[T]he police can be said to have seized an individual 'only if, in view of all of the circumstances surrounding the incident, a reasonable person would have believed that he was not free to leave.'" (quoting *United States v. Mendenhall*, 446 U.S. 544, 554 (1980) (plurality opinion))); *Terry v. Ohio*, 392 U.S. 1, 19 (1968) ("Only when the officer, by means of physical force or show of authority, has in some way restrained the liberty of a citizen may we conclude that a 'seizure' has occurred."). [iii]

The court of appeals then stated, even if a seizure occurred in Overton's case, the issue is whether that seizure is reasonable or unreasonable under the Fourth Amendment.

The court then examined facts relevant to whether the seizure was reasonable. The court noted that the fire fighters detained Overton, who was unconscious upon their arrival, to render medical treatment, not to obtain evidence against him or arrest him. The court then held that this brief detention that was intended to render medical aid for Overton's benefit, was not unreasonable under the Fourth Amendment. As such, since the detention led to the discovery of the firearm, the firearm was admissible.

Note: Court holdings can vary significantly between jurisdictions. As such, it is advisable to seek the advice of a local prosecutor or legal adviser regarding questions on specific cases. This article is not intended to constitute legal advice on a specific case.

Citations

i. No. 13-3274 (6th Cir. 2014 Unpublished)

ii. Id. at 3

iii. Id. at 11

Policy #	
Internet Use & Online Social Networking	
This policy is for internal use only and does not enlarge an employee's civil liability in any way. The policy should not be construed as creating a higher duty of care, in an evidentiary sense, with respect to third party civil claims against employees. A violation of this policy, if proven, can only for the basis of a complaint by this department for non-judicial administrative action in accordance with the laws governing employee discipline.	
Applicable State Statutes:	
CALEA Standard:	
Date Implemented:	Review Date:

I. Purpose: The purpose of this policy is to direct the employees of this agency with respect to the use of the internet, the world-wide web, and social networking as a medium of communication impacting this department.

II. Policy: The internet, blogs, twitter, the worldwide web, social networking sites and any other medium of electronic communication shall not be used in a manner which is detrimental to the mission and function of this agency.

It is essential for every employee of this agency to recognize that the proper functioning of any law enforcement agency relies upon the public's confidence and trust in the individual officers and this agency to carry out the law enforcement function. Therefore, any matter which brings individual employees or the agency into disrepute has the corresponding effect of reducing public confidence and trust in our agency, thus, impeding our ability to work with and serve the public. Professionalism is the most significant factor in high level performance which in turns builds the public confidence and trust. While employees have the right to use personal/social networking pages or sites, as employees of this agency, they are public servants who are held to a higher standard that the general public with regard to standards of conduct and ethics. As such, the policy of this agency is to maintain a level of professionalism in both on-duty and off-duty conduct that fulfills the mission of our agency. Any publication, through any medium which is potentially adverse to the operation, morale, or efficiency of this agency will be deemed a violation of this policy.

III. Procedure:

A. Employees of this agency are prohibited from using agency computers for any unauthorized purpose including surfing the internet or participating in social networking sites.

B. Employees of this agency are prohibited from posting, or in any other way broadcasting, without prior agency approval, information on the internet, or other medium of communication, the business of this agency to include but not limited to:

a. Photographs/images relating to any investigation of this agency.

b. Video or audio files related to any investigation of this agency

c. Video, audio, photographs, or any other images etc. which memorialize a law enforcement related action of this agency.

d. Logos/Uniforms/Badges or other items which are symbols associated with this agency.

e. Any other item or material which is identifiable to this agency.

C. Employees of this agency who utilize social networking sites, blogs, twitter or other mediums of electronic communication in their off-duty time shall maintain an appropriate level of professionalism and appropriate conduct so as not to broadcast in a manner which is detrimental to the mission and function of this agency.

a. Employees shall not use references in these social networking sites or other mediums of communication that in any way represent themselves as a employee of this agency without prior agency approval. This shall include but not be limited to:

i. Text which identifies this agency.

ii. Photos that depict the logos, patches, badge or other identifying symbol of this agency.

iii. Accounts of events which occur within this agency.

iv. Any other material, text, audio, video, photograph, or image which would be identifiable to this agency.

b. Employees shall not use a social networking site or other medium of internet communication to post any materials of a sexually graphic nature.

c. Employees shall not use a social networking site or other medium of internet communication to post any materials which promote violence or weaponry.

d. Employees shall not use a social networking site or other medium of communication to post or broadcast any materials which would be detrimental to the mission and function of this agency.

D. Employees of this agency are prohibited from using their title as well as any reference to this agency in any correspondence to include emails, postings, blogs, twitter, social network sites such as Facebook, unless the communication is of an official nature and is serving the mission of this agency. This prohibition also includes signature lines in personal email accounts. An employee may seek agency approval for such use.

E. New employees: All candidates seeking employment with this agency shall be required to complete an affidavit indicating their participation in any social networking sites. This affidavit shall include the name of the sites. The candidate shall provide the agency with access to their site as part of any background examination.

F. Administrative Investigations: Employees who are subject to administrative investigations may be ordered to provide the agency with access to the social networking site when the subject of the investigation is directly, narrowly, and specifically related to the employee's performance or ability to perform his or her function within the agency or when the subject of the investigation is potentially adverse to the operation, morale, or efficiency of the agency.

INTERNET & ELECTRONIC COMMUNICATION POLICY OF [CITY/COUNTY]

1. Policy Statement. Computers and computer-related services are made available to departments and employees of the [CITY/COUNTY] for business-related purposes. In particular, Internet and electronic mail (email) services are provided to support open communications and exchange of information and the opportunity for collaborative government-related work. While [CITY/COUNTY] believes that computers and computer-related services, including Internet and email, are essential tools for its departments and employees, access to such services is a revocable privilege. As such, conformance with acceptable use, as expressed in this Policy, is required. Departments of [CITY/COUNTY] are expected to maintain and enforce this Policy.

2. Relationship to Other Policies. This Policy supplements any and all [CITY/COUNTY] policies relating to workplace harassment, discrimination, retaliation, conflicts of interest, discipline and discharge, records retention, and Open Meetings Act compliance.

3. No Expectation of Privacy. [CITY/COUNTY] computers and any data stored in them are the property of [CITY/COUNTY] and may be accessed at any time by authorized officials of [CITY/COUNTY]. Employees shall not expect privacy in the use of [CITY/COUNTY] computers. [CITY/COUNTY] may, without notice, monitor Internet usage and/or email and review computer files to ensure that computers are not being used for impermissible purposes.

4. Public Records. Many emails and other electronic files constitute public records for purposes of state record retention laws. As such, whether a given email or electronic file is subject to a retention schedule must be determined by its content rather than its format. As a general rule, any email or other electronic file which is a substitute for a letter, memorandum, notice, report, or other traditional record that would be subject to a particular retention schedule, then it too is subject to the schedule. Conversely, if the email or other electronic file is merely transitory, it need not be retained beyond its useful life (e.g., listserv messages, meeting notices, general staff announcements, invitations to events, etc.). Users of [CITY/COUNTY] computers and other computer-related services must also bear in mind that all emails and other electronic files are generally subject to disclosure under the Open Records Act.

5. Acceptable Uses. The following constitute acceptable uses of the Internet and email made available to employees by [CITY/COUNTY].

- Communication and information exchange directly related to the user's duties and responsibilities as an employee of [CITY/COUNTY] or the mission and function of his/her department.
- Communication and exchange for the user's professional development as an employee of [CITY/COUNTY], to maintain currency of his/her relevant training or education, or to discuss issues related to his/her research, projects, or programs as an employee of [CITY/COUNTY].
- Use in applying for or administering grants or contracts for [CITY/COUNTY]'s research or programs.
- Use for advisory, standards, research, analysis, and professional society activities related to the user's duties and responsibilities as an employee of [CITY/COUNTY].
- Announcements of new [CITY/COUNTY] regulations, ordinances, procedures, policies, rules, services, programs, information, or activities.
- Any other authorized [CITY/COUNTY]-related administrative communications not requiring a high level of security.

6. Specifically Unacceptable Uses. The following constitute unacceptable uses of the Internet and email made available to employees by [CITY/COUNTY] and may subject an employee to disciplinary action, up to and including termination of employment.

- Visiting inappropriate web sites (erotica, hate groups, etc.).
- Unauthorized attempts to access any computer or network.
- Sending or posting threatening or otherwise inappropriate messages.
- Sending or posting racially and/or sexually harassing messages or images, sending or posting any sexually suggestive or explicit messages, or any other use violative of [CITY/COUNTY] policies regarding workplace harassment, discrimination, and/or retaliation.
- Accessing or copying confidential and/or proprietary software, program, or other electronic files without permission.
- Sending or posting confidential information without authorization.
- Downloading, uploading, or sending viruses or other malicious files or programs.
- Opening or sending emails or other electronic files that may endanger [CITY/COUNTY] computers and/or network.
- Using the Internet and/or email for any purpose which violates a federal, state, or local law.
- Using the Internet and/or email for any private business or other for-profit activities unrelated to the user's duties and responsibilities as an employee of [CITY/COUNTY].
- Accessing, downloading, or sending computer games that have no bearing on the user's duties and responsibilities as an employee of [CITY/COUNTY], recognizing that some games designed to teach, illustrate, train, or simulate agency-related issues may be acceptable.
- Accessing, copying, or modifying electronic files stored within [CITY/COUNTY] computers outside of the user's duties and responsibilities as an employee of [CITY/COUNTY] without authorization.
- Disclosing or exchanging passwords or seeking or obtaining passwords of other employees of [CITY/COUNTY] or other authorized users of [CITY/COUNTY] computers and computer-related services.
- Representing oneself as another user, either on [the CITY/COUNTY] internal network or elsewhere on the Internet, without authorization.
- Intentionally developing programs designed to harass other users or infiltrate a computer or computing system and/or damage or alter the software components of same.
- Fundraising or public relations activities not specifically related to the user's duties and responsibilities or to [CITY/COUNTY] approved activities.

7. Procedures. Department heads, or their designees, are responsible for their employees' compliance with the provisions of this Policy and for promptly investigating non-compliance. Suspension of service to users may occur when deemed necessary to maintain the operation and integrity of [CITY/COUNTY] network. User accounts and password access may be withdrawn without notice if a user violates the acceptable use policy. Disciplinary action up to and including termination of employment may be imposed depending on the severity of the violation. Criminal or civil action against users may be initiated when laws are violated.

8. Guidelines. The following additional guidelines apply to uses of the Internet and email made available to employees by [CITY/COUNTY].

- *Checking for viruses*. Any software obtained from outside [CITY/COUNTY] shall be scanned prior to use for viruses and other malicious files or programs.

- *Contractors.* Contractors and other non-[CITY/COUNTY] users may be granted access to [CITY/COUNTY]-provided Internet and/or email services at the discretion of the department head. Acceptable use by such users is the responsibility of [CITY/COUNTY] contract administrator, who is expected to provide such users with this policy.

- *Passwords.* Use passwords associated with the [CITY/COUNTY] information system only on that system. When setting up an account at a different information system that will be accessed using the Internet, choose a password that is different from ones used on [CITY/COUNTY] information systems. Do not use the same password for both local and remote Internet-accessed systems. If the password used at the remote, Internet-accessed remote site were to be compromised, the different password used locally would still be secure. Passwords should not be so obvious so that others could easily guess them, and passwords should be changed at least every sixty days.

- *Logging off.* Always make a reasonable attempt to complete the logoff or other termination procedure when finished using a remote, Internet-accessed system or similar resource. This will help prevent potential breaches of security.

- *Email Security*. Always remain mindful that unencrypted email sent or received outside any department and on the Internet cannot be expected to be secure.

- *Large File Transfers and Internet Capacity*. The Internet connection is a shared resource. While routine email and file transfer activities generally will not impact other users, large file transfers and intensive multimedia activities will impact the service levels of other users. Users contemplating file transfers of over ten megabytes per transfer or interactive video activities shall, to be considerate of other users, schedule these activities early or late in the day or, if possible, after business hours.

- *Conduct & Etiquette*. Know and follow generally accepted Internet and email etiquette. Refrain from language or other uses of the Internet and email that reflect poorly on [CITY/COUNTY].

- *Correspondence with Legal Counsel / Disclaimer*. Any email or other correspondence sent to the [CITY ATTORNEY/COUNTY ATTORNEY] or other legal counsel for [CITY/COUNTY], if sent for the purpose of assisting legal counsel in providing legal advice to [CITY/COUNTY], must include the following disclaimer:

  > "This communication and all attachments may contain privileged and confidential legal communications/attorney work product intended solely for the use of the addressee. If you are not the intended recipient, any reading, distribution, copying or other use of this communication and/or any attachments hereto is prohibited and you should delete this message from all locations, and advise the sender at [INSERT TELEPHONE NUMBER AND/OR EMAIL ADDRESS]. Thank you."

9. Use of Computer Software.

- In compliance with federal copyright laws, [CITY/COUNTY] will not participate in or condone the illegal duplication of licensed microcomputer software. Such activity is strictly prohibited on [CITY/COUNTY] premises and/or computers. [CITY/COUNTY] does not own the copyright to any software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it for use on more than one computer.

- With regard to use on local area networks or on multiple machines, [CITY/COUNTY] employees and other authorized users shall use the software only in accordance with the license agreement.

- [CITY/COUNTY] employees are required to promptly report any misuse of software or related documentation within [CITY/COUNTY] to their department head or to [TITLE OF APPROPRIATE OFFICIAL].

Providing Loss Prevention,
Loss Control & Health
Promotion Services for
Local Governments

Property & Liability Risks
Employee Safety
Health & Wellness

Local Government
Risk Management Services
3500 Parkway Lane • Suite 110
Norcross, Georgia 30092

A Service Organization of the Association County Commissioners of Georgia and the Georgia Municipal Association

This Month:

Internet and Electronic Communication Policies
Seizure and Fire Fighters

GEORGIA MUNICIPAL ASSOCIATION

ACCG
Advancing Georgia's Counties.