SMITH HAUGHEY
RICE & ROEGGE
ATTORNEYS AT LAW

The Technology Issue

Governmental Liability in the High Tech Environment

January 2012

Introduction

By Karl W. Butterer, Attorney

It is difficult to overstate the impact of evolving electronic technology on our everyday lives. The internet, e-mail, the mobile phone, global position satellite (GPS) capability, the storage of information in electronic format, and the rise of social media have profoundly impacted the world around us. In 1993, the internet carried an estimated 1% of the information flowing through two-way telecommunication. According to *Science*, by 2007 more than 97% of all telecommunicated information was carried over the internet. Pew Internet reports that by 2009, 74% of American adults were using the internet. Eighty-three percent of adults have cell phones or smart phones and, among them, 35% have accessed the internet via their phone. Mobile phones increasingly include texting and GPS capabilities. Social networking – which permits a user to post videos, photographs and text on the internet with a click – now accounts for 22% of all time spent online in the U.S., according to Nielsen. Facebook, the most popular social networking site, reports that it will have an estimated 800 million users this year. GPS systems are increasingly included in vehicles.

Governmental units may question their legal duties and limitations in this information-rich, instantaneous and electronic environment. To complicate matters, some of those duties and limitations are unique to governmental agencies, while some are applicable to all employers, and to all individuals saving or accessing electronically stored information. Common questions include:

In this issue:

"Limitations on Government Agencies in Cyberspace".....*Pg. 2*

"WHEN to Start Saving Electronic Information is Just as Important as WHAT You Save"…….. *Pg. 5*

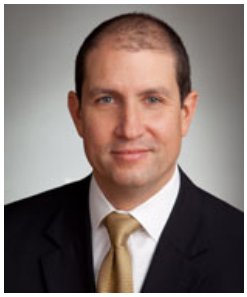
"Use of Global Position Satellite Technology by Local Government Agencies……..….*Pg. 5*

"Attorney Profile: Karrie Zeits"……...…….*Pg. 8*

- May a government agency secretly view the e-mail of an employee?
- May the government track the location and travel habits of its employees at work or away from work?
- What are the duties of governmental agencies

to save electronically stored information?
- May a government employer access a social networking page to investigate an employee?
- May a government agency terminate an employee for blogging about internal office politics?

While the answers to these questions are too complex and fact-dependent to answer in full in these few pages, the purpose of this "Legal Alert" is to offer some advice on legal developments in these areas.



About the Author: Karl Butterer has litigated on behalf of governmental agencies and their employees for 17 years. He has successfully defended clients in cases involving state tort claims, 42 U.S.C. Section 1983, Title VII, the Whistle Blower Protection Act, the Elliott Larsen Civil Rights Act, 42 U.S.C. Section 1985, and the Michigan Constitution, among others. For more information on Karl, please visit his attorney profile at shrr.com.

Limitations on Government Agencies in Cyberspace

By Karl W. Butterer, Jr. and Charissa C. Huang, Attorneys

Government Searches of Electronic Information

The United States Constitution, which was written approximately 200 years before the wide-use of computer technology, provides the basic framework from which to analyze the limitations on the government's search of a person's use of a computer, a mobile phone, or the internet. The Fourth Amendment to the Constitution protects "[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." A 1967 legal case, *Katz v United States*, states "[t]he touchstone of Fourth Amendment analysis is whether a person has a constitutionally protected reasonable expectation of privacy." The *Katz* Court explained:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

An individual's constitutionally protected privacy may extend to information located on a computer, a phone, or even displayed on a website (in some situations).

In the employment context, one way for a governmental agency to avoid a claim that it made an unlawful search or seizure of electronic information is to make a clear disclosure that the employee's use of technology will be monitored. In *U.S. v Simons*, the government employer had an internet policy which clearly stated that the employer would "audit, inspect, and/or monitor" employee's use of the internet, including all file transfers, all websites visited and all e-mail messages "as deemed appropriate." The federal court determined that the employees had been placed on notice that they could not reasonably expect that their internet activity would be private. In contrast, in *U.S. v Slavina*, the government employer violated the Fourth Amendment when it viewed files which were stored on the employee's computer because the governmental agency did not have a policy placing the employee on notice that

his computer usage would be monitored, or that other employees had routine access to his computer.

The motivation for the governmental unit's surveillance of an employee's technology usage also has an impact on whether the surveillance will be deemed reasonable. In *City of Ontario, Val. v Quaon*, a police officer sued the municipality for reviewing text messages he sent and received on a city-issued pager. The court found that the review did not violate the Fourth Amendment because the investigation was not motivated by a desire to uncover wrongdoing, but rather to determine whether the employee's repeated exceeding of the monthly character limit was the result of work-related use or personal use.

The Stored Communications Act

"It is important for municipal employers to recognize the potential for liability based upon the procedures through which they monitor employee internet activity."

It is important for municipal employers to recognize the potential for liability based upon the procedures through which they monitor employee internet activity. The Stored Communications Act makes it an offense to "intentionally access[] without authorization a facility through which an electronic communication service is provided... and thereby obtain[]... access to a wire or electronic communication while it is in electronic storage in such system." The Act excepts from liability, however, "conduct authorized... by a user of that service with respect to a communication of or intended for that user."

Employers may be liable under federal law for monitoring employee internet activity when, in the course of their surveillance, the employer improperly accesses password-protected websites. In *Pietrylo v Hillstone Restaurant Group*, the court affirmed an award of compensatory and punitive damages where the defendant restaurant managers violated the Stored Communications Act by improperly accessing an employee's private password-protected, invitation-only MySpace chat room that was created during the employee's "off duty" time as a forum for employees to talk about the "crap/drama/and gossip" at work. The managers used a password obtained from another employee who testified that she "would have gotten in trouble" if she had not let the managers use her password. Accordingly, the court held her consent may have been coerced. As a result, the restaurant chain was held liable because its managers violated the Stored Communications Act.

The Ninth Circuit came to a similar conclusion in *Konop v Hawaiian Airlines, Inc*. In that case, *Konop*, an airline pilot, created and maintained a password protected website where he posted bulletins critical of his employer. The employer's Vice President asked two employees for their names to access the site, and both employees agreed. Since the court found no evidence in the record that the two employees who lent their names to the vice president had ever actually used the website, it concluded that the employees were not "users" within the meaning of the Act. Thus, the Court of Appeals reversed the district court's grant of summary judgment in favor of the defendant employer.

Thus, the upshot of *Pietrylo* and *Konop* is that while employers may be able to monitor password protected websites created by employees, they should be careful to obtain access through noncoercive means and through employees that have previously used the websites.

Social Networking, Blogging and the First Amendment

The rise of social networking and blogging has increased opportunities for government employees

to engage in public speech regarding the operations of the governmental agencies which employ them. Some of the employee's speech may be critical of the governmental agency, or may even go so far as to interfere with the efficient operations of the agency. Some of the employee's speech may be protected by the First Amendment, while some of it may not be protected. Accordingly, it is important for a governmental agency to review under what circumstances it may take adverse action against an employee for engaging in speech about the governmental agency.

The United States Supreme Court has long recognized that public employees do not forego all the protection of the First Amendment by virtue of working for the government. The Court has sought to balance the interests of government employees' right to free speech with the government employer's interest in exercising some degree of control over their employees' words and actions in order to ensure the efficient provision of public services. Thus, the court held in *Carcetti v Ceballos* that "[s]o long as employees are speaking as citizens about matters of public concern, they must face only those speech restrictions that are necessary for their employers to operate efficiently and effectively."

"…it is important for a governmental agency to review under what circumstances it may take adverse action against an employee for engaging in speech about the governmental agency."

Municipal employers should consider potential liability under the First Amendment before taking adverse employment action based upon an employee's posts on the internet or social networking sites. As described in *Connick v Myers,* the determination of whether an employee's speech through internet posts would constitute speech on matters of "public concern" depends on the content, form, and context of a given statement, as revealed by the whole record. Further, *Kearney v City of Bridgeport Police Dept*. explains that speech is a matter of public concern if it relates "to any matter of political, social, or other concern to the community." However, *Connick* also states that the First Amendment does not require a public office to be run as a roundtable for employee complaints over internal office affairs. Thus, a municipal employer should consider these factors in addressing whether adverse employment action based upon an employee's internet posts would expose it to a claim that it acted in retaliation against a plaintiff employee for exercising her First Amendment rights.

Government Employee Rights to Organize

Before taking adverse employment action based on an employee's internet activity, municipal employers should also consider the potential for liability for violating workers' rights to organize, bargain collectively, and engage in concerted activity for their mutual aid and protection under Michigan's Public Employment Relations Act. Consideration of liability based upon violation of workers' right to organize is especially important in situations where a municipal employee has created a website as a "forum" for employees to discuss work-related subjects.

For example, in *City of Detroit v Detroit Police Officers Assoc*, a police officer, Officer Bennett, created a website to provide a forum for police officers to express concerns regarding the police department. It included some comic relief and "edgy" criticism of departmental officials and a "guest book", which allowed anyone to express their thoughts. The Chief suspended Bennett with pay and told Bennett that the website contained racial materials and, if he did not shut down the website, he would be suspended without pay. Officer Bennett continued to operate the website.

Eventually, Bennett's suspension was changed to one without pay, with the approval of the Detroit Board of Commissioners. The Detroit Police Officers Association (DPOA) then brought a Michigan Employment Relations Commission (MERC) action against the Chief, the City of Detroit, and the city mayor.

The administrative law judge found that the respondent violated the Public Employment Relations Act by suspending Officer Bennett for engaging in protected activity under MCL 234.210(1) which provides that "[i]t shall be unlawful for a public employer or an officer or agent of a public employer (a) to interfere with, restrain or coerce public employees in the exercise of their rights guaranteed in section 9." MCL 423.209 provides:

> It shall be lawful for public employees to organize together or to form, join or assist in labor organizations, to engage in lawful concerted activities for the purpose of collective negotiation or bargaining or other mutual aid and protection, or to negotiate or bargain collectively with their public employers through representatives of their own free choice.

On appeal, the court found that Officer Bennett was engaged in protected activity under Section 9. Since there was evidence that Bennett was not given an option to remove objectionable material, but rather was told to shut down the website or face a suspension without pay, the court held that the evidence supported an inference that the plaintiff's right to engage in lawful concerted activities was adversely affected by the suspension. In affirming the recommended order, the court opined that "employees are not precluded from seeking to improve terms and conditions of employment, or to otherwise improve their lot as employees, through channels outside the employee-employer relationship."

Conclusion

The internet, social networking, blogging and other computer technology have vastly expanded the type and amount of electronic information flowing from, between and to governmental agencies, their employees, and the world at large. Governmental agencies may be interested in searching or monitoring this electronic information. However, the United States Constitution, as well as both federal and state statutes, place limitations on how and why the government may gain access to this information. The lawyers at Smith Haughey Rice & Roegge are available to partner with you to navigate this evolving legal environment.

Karl can be reached directly at 616-458-9294 or kbutterer@shrr.com. Charissa can be reached directly at 616-458-3443 or chuang@shrr.com.

WHEN to Start Saving Electronic Information: It is Just as Important as WHAT You Save

By Kristen E. Ray, Attorney

"ESI" and "electronic discovery" are becoming common terms throughout various industries. Organizations involved in lawsuits have learned that they must instruct their IT departments and employees to put a "hold" on deleting electronically stored information in case that information becomes necessary during the litigation process.

What may not be as clear is <u>when</u> to start the "hold" on deleting this information. The common misperception is that the "hold" should begin when

a lawsuit is filed. Although this makes sense, this is not what the law requires. In some instances, if the "hold" is not implemented timely and appropriately, a court could issue sanctions against the party – including payment of fines, loss of use of some important information, adverse jury instructions, and/or, more severely, a default against that party in the litigation.

There is little Michigan case law regarding when a party should begin the "hold." However, with regard to ESI and electronic discovery disputes, Michigan courts have relied heavily upon Federal cases. The Michigan Court Rules regarding ESI closely model the Federal court rules. **It is advised, therefore, to start the "hold" when litigation is "reasonably anticipated."** For example, this may include a notice of intent to sue which a plaintiff must give a governmental agency in highway defect cases, a letter threatening suit, or an informal complaint. Once this triggering event takes place, a "hold" must be implemented. All key personnel with knowledge or information regarding the subject matter of the possible litigation, including IT staff, must be notified that a "hold" must go into effect immediately.

Kristen can be reached directly at 616-458-9418 or kray@shrr.com.

Use of Global Position Satellite Technology by Local Government Agencies

By Karl W. Butterer and Michael D. Shelton, Attorneys

Global Position Satellite (GPS) technology is commonly installed in mobile phones and vehicles, and allows an employer to identify and track the location of equipment and employees with relative ease. Despite the benefits of GPS, there are several things a governmental agency should consider before taking advantage of this technology. The use of GPS by government agencies may give rise to constitutional challenges for "unreasonable searches," or may violate state privacy laws. Additionally, subjecting employees to GPS tracking could be challenged under an applicable collective bargaining agreement or the Michigan Public Employment Relations Act (PERA), MCL 423.201 *et seq,* which obligates employers to negotiate with union-represented employees regarding working conditions.

U.S. v Jones

In the recent case of *United States v. Jones*, the United States Supreme Court has been presented with the question of whether or not the government's use of GPS tracking devices, installed without a warrant on a person's vehicle in order to track the person's movements for almost an entire month, constitutes an unreasonable search in violation of the Fourth Amendment of the United States Constitution. In oral argument, the Court questioned whether or not the consent of the owner of the vehicle would make the attachment of a tracking device constitutional, or whether the vehicle operator's consent was needed. The Court has not issued a decision on this case yet, but regardless of how the decision turns out, government employers should view the court's concerns and inquiries as guidelines when determining whether or not, and how, to implement GPS technology in the workplace.

Among the things to consider:

- On what equipment will the GPS technology be installed, e.g.: mobile phone or a vehicle?
- Is it the agency's equipment or the employee's?

- Should the employee be informed of the GPS tracking device?
- Is it likely that the equipment will monitor an employee's movements outside of work hours?
- If so, will it monitor private activities inside the home or otherwise?

Further consideration should be given to how the information will be used. Will the information be used solely for the purpose of improving the agency's performance and efficiency, or will the information be used for disciplinary purposes when a violation of agency policy is found? The answers to these questions may affect not only the lawfulness of the GPS monitoring, but also the morale of the employees and their acceptance or aversion to the new monitoring.

There are very few reported cases dealing directly with these issues. In a pair of Connecticut cases, *Vitka v City of Bridgeport* and *Gerardi v City of Bridgeport*, the plaintiffs were fire inspectors for the city. The city installed GPS on its vehicles, but never informed the employees who drove them. Based on the information obtained by the GPS, the plaintiffs were fired. The court appeared to decide the case on Fourth Amendment grounds. The court held that, "monitoring revealing information that could be seen in plain view" was not a search, in violation of the constitution and because the city vehicle was being monitored while in plain view there could be no problem with the city tracking its vehicle even if the driver did not know.

Michigan Privacy Laws

Michigan has statutory laws which make it a crime to install or place a "tracking device" on a motor vehicle for purposes of surveillance. However, it is not entirely clear whether this law would prevent a government employer from placing a GPS device on a vehicle which it owns, but that is operated by an employee.

The statute initially appears to allow such activity because a person only violates the law when he "installs or places a tracking device... in or on a motor vehicle without the knowledge and *consent of the owner*... [or] tracks the location of a motor vehicle... without the knowledge and *consent of either the owner or the authorized operator*." The plain language indicates that the owner can give permission and the vehicle operator is not required to know of the device or the tracking. However, it is not certain that the same activity will not violate a different section of the privacy statute. The statute also makes it a misdemeanor to trespass on property owned *or under the control* of any other person, to subject that person to... surveillance." The term "surveillance" means to "secretly observe the activities of another person for the purpose of spying upon *and* invading the privacy of the person observed." (Emphasis added.) Does the tracking of the location of a vehicle by the owner, or the compilation of historical information about the movement of the vehicle, constitute an invasion of the operator's privacy when the movements of the vehicle are otherwise open to the public to observe? Is the analysis different for a mobile phone because mobile phones are not covered by the statute which permits the tracking of motor vehicles by their owners? These issues have yet to be resolved by the courts.

Michigan Laws Governing Labor Relations

Michigan's PERA governs labor relations for public employees in Michigan and is similar to the National Labor Relations Act (NLRA), which regulates labor relations for private sector employees. Since PERA rights are similar to NLRA rights for private sector employees, decisions under the NLRA often provide guidance regarding interpretation of PERA.

Of particular importance is Section 15 of PERA which, like the NLRA, imposes upon employers the duty to collectively bargain with the employees' representatives in good faith. Because of the similarity between the federal and state labor laws, some NLRA cases can be used to illustrate the potential problems that can arise in employment relationships governed by collective bargaining agreements.

If the employees are unionized, the Collective Bargaining Agreement (CBA) should be reviewed to ensure that the terms of the agreement do not prohibit such monitoring of the employees in the workplace. Even if the CBA does not prohibit the use of GPS devices to track equipment or employees, consideration should be given to the question of whether or not this is a management decision that can be made unilaterally, or a change in working conditions that must be negotiated with the union.

"If the employees are unionized, the Collective Bargaining Agreement should be reviewed to ensure the terms of the agreement do not prohibit such monitoring of the employees in the workplace.

In *Otis Elevator Co v Local 1, International Union of Elevator Constructors*, Otis Elevator Co., decided to install GPS devices in the company vehicles that the employees drove to work and routinely drove home. The Otis employees were concerned about "'big brother' monitoring" and refused to drive the vehicles home after work, opting instead to leave them on Otis' property. Some employees even disabled the GPS devices in the vehicles. Otis' stated intent was to improve efficiency, reduce insurance costs, and hasten the recovery of stolen vehicles.

The dispute went to arbitration, where the arbitrator determined that the language of the CBA allowed Otis to make such changes unilaterally, and further held that Otis could order its employees to drive the vehicles home even when not compensated for the time. The arbitrator reached this conclusion based on the ambiguity of the CBA, which gave Otis the ability to require that employees use company vehicles whenever they are provided, and past practice of the employees always driving the vehicles home after work.

The U.S. District Court for the Southern District of New York affirmed the arbitrator's decision based on the express language of the CBA which allowed for technology upgrades for purposes of efficiency. The court further held that the language in the CBA was reasonably ambiguous and the past practice was a sufficient basis for interpreting the CBA to require employees to drive the vehicles home after work.

In 2010, Verizon New England, Inc. experienced some disruption at workplaces resulting from new policies requiring employees to carry cell phones with GPS tracking devices. As in *Otis*, employees were concerned that the cell phones could be used to track their movements and conduct while they were off work. The employees, who were members of the International Brotherhood of Electrical Workers (IBEW), and Verizon New England, Inc. both filed suit. In *Haggins v Verizon New England, Inc*, the employees claimed that the use of the GPS in cell phones to track the employees was in violation of state privacy laws and was an unfair labor practice under the NLRA. As a result of some alleged concerted action resulting in a temporary work stoppage and mass refusal to perform overtime or to carry the cell phones with tracking devices, Verizon New England, Inc. filed suit against the IBEW, Local 2322 alleging that the local labor union had breached the collective bargaining agreement (*Verizon New England, Inc v local No 2322, International Brotherhood of Electrical Workers*).

While the courts did not decide the issue of whether policies that subject employees to tracking would be a mandatory bargaining item, these *Verizon New England, Inc* cases and *Otis* demonstrate the potential disruption and loss of productivity which can occur, in response to GPS monitoring; not to mention the financial costs of grievances, unfair labor practices and arbitration proceedings.

Still it is undeniable that GPS has great potential, and an employer may be able to benefit greatly from using it. Some employers have successfully used GPS recordings to substantiate a denial of unemployment insurance payments after an employee was discharged for violating company policy, as in *Wilson v Unemployment Insurance Appeal Board*. The employee used a company vehicle for personal use, and the GPS reports revealed this fact to the company. During the employee's appeal to the company's denial of unemployment insurance payments, the GPS reports were used to confirm that the employee was fired for just cause.

In another case, *Spinks v Twp of Clinton*, the police department used GPS devices to conduct an internal investigation of its own officers in an effort to catch employees falsifying their time reports and being idle on the job. Such action was held to be lawful, and the prosecutor who ordered the investigation was protected by qualified immunity. However, had the conduct violated a well established fundamental right—such as the Fourth Amendment—the prosecutor, or whoever it is making the decision, could have lost his immunity.

Conclusion

Whether, and how, a government agency should install GPS tracking devices on vehicles, cell phones or other devices is a complicated question; the answer to which involves an analysis of the Fourth Amendment, state privacy laws, employment and labor laws, as well as employee relations. If your government agency is considering the placement of such devices, the attorneys at Smith Haughey Rice & Roegge can provide you legal advice and consultation to help make this important decision.

Karl can be reached directly at 616-458-9294 or kbutterer@shrr.com. Mike can be reached directly at 616-458-0268 or mshelton@shrr.com.

Attorney Profile: Karrie A. Zeits

The Governmental Law Practice Group at Smith Haughey is happy to announce the addition of Karrie Zeits.

Karrie Zeits has 11 years of experience working for municipalities and other governmental agencies in northern Michigan . Prior to joining Smith Haughey, Karrie was the City Attorney with the City of Traverse City. In this role, she was the chief legal advisor to the City Commission, City Manager, and all city officers and employees. She also provided counsel for other governmental agencies such as the Downtown Development Authority and the City of Traverse City and Charter Township of Garfield Recreational Authority.

Karrie has worked closely with government officials at all levels. Her profound and in-depth knowledge of municipal operations and regulations

offer unique insight to her clients both in and out of government. On a daily basis, Karrie advises municipalities, government officials, and employees on general administrative and governance issues, policies, and laws and in matters related to employment and labor relations, contract negotiations, the Freedom of Information Act, Open Meetings Act, and board governance. She also counsels her clients on issues related to zoning and real estate transactions. Karrie litigates on behalf of her clients in civil court and administrative tribunals, including the Michigan Tax Tribunal.

Karrie earned a Bachelor's degree from Albion College and a Juris Doctor from Willamette University College of Law. She is a member of the State Bar of Michigan (where she serves as a board member for the Section on Public Corporation Law), Grand Traverse-Leelanau-Antrim Bar Association, Michigan Association of Municipal Attorneys, and the Women Lawyers Association. Karrie is active in the legal profession and the Traverse City community. She previously taught Legal Research and Writing at Northwestern Michigan College.

Karrie can be reached directly at kzeits@shrr.com or 231-486-4521.

SHRR Governmental Law Attorneys

Charles F. Behler 616.458.6245 cbehler@shrr.com	**Karl W. Butterer** 616.458.9294 kbutterer@shrr.com	**William L. Henn** 616.458.5464 whenn@shrr.com	**Charissa C. Huang** 616.458.3443 chuang@shrr.com
Charles B. Judson 231.929.4878 cjudson@shrr.com	**Todd W. Millar** 231.486.4512 tmillar@shrr.com	**Craig R. Noland** 616.458.9466 cnoland@shrr.com	**Robert W. Parker** 231.486.4504 rparker@shrr.com
Michael D. Shelton 616.458.0268 mshelton@shrr.com	**Robert C. Stone** 616.458.3622 rstone@shrr.com	**D. Adam Tountas** 616.458.0437 tountas@shrr.com	**Karrie A. Zeits** 231.486.4521 kzeits@shrr.com