July/August 2016

IMLA

Municipal Lawyer

THE JOURNAL OF LOCAL GOVERNMENT LAW

SPECIAL TECH ISSUE

Public Safety Technologies: The Fourth Amendment Balancing Act

A Wealth of Information: Data Security and Local Governments

The Good, the Bad and the Ugly: Driverless Vehicles and Municipalities

LISTSERV: The First Amendment and the Right to Toss Pizzas

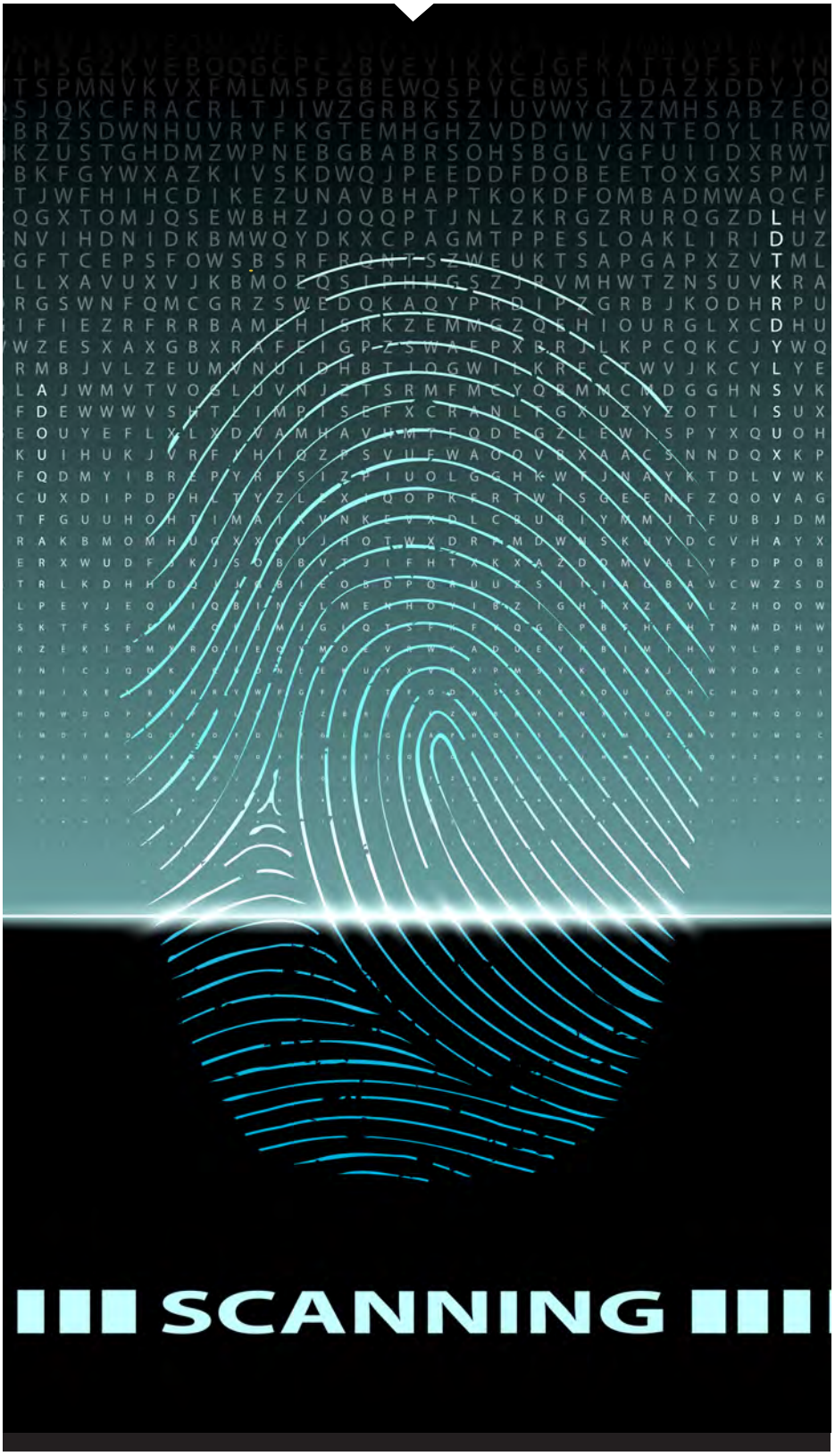
FEDERAL: The FDA's First E-Cigarette Regulation

SECOND LOOK: Objecting to Requests for Production

AMICUS CORNER: A Focus on Recent Qualified Immunity Cases

INSIDE CANADA: Cases of Interest

IMLA: Board of Directors Election





Have a job position that you need to fill?

Use IMLA's job board to reach top quality candidates.

Take advantage of our 20% discount until August 31!

Promo code: 5BA7HYK2.

.



IMLA

Phone: 202.466.5424
Fax: 202. 785.0152
E-mail: info@imla.org
Website: www.imla.org

7910 Woodmont Avenue
Suite 1440
Bethesda, Maryland 20814

PRESIDENT
Herbert W. A. Thiele
County Attorney
Leon County, FL

PRESIDENT-ELECT
Mary Ellen Bench
City Solicitor
Mississauga, ON, Canada

IMMEDIATE PAST PRESIDENT
G. Foster Mills
Managing Attorney (retiresd)
New York City, NY

TREASURER
Andrew J. Whalen, III
City Attorney
Griffin, GA

GENERAL COUNSEL
EXECUTIVE DIRECTOR
Charles Thompson, Jr.
IMLA
Bethesda, MD

DIRECTORS
Barbara A. Adams
Village Attorney
Kenilworth, IL

Patrick Baker
City Attorney
Durham, NC

Marianne Landers Banks
Interim City Attorney
Springfield, MO

A. René Broker
Borough Attorney
Fairbanks North Star, AK

Tyrone E. Cooper
City Attorney
Beaumont, TX

Robert S. Croom
Deputy General Counsel
South Carolina Association of Counties

Gary Ebert
Director of Law
Bay Village, OH

Wayne Esannason
Village Attorney
Scarsdale, NY

Cathy D. Hampton
City Attorney
Atlanta, GA

Douglas C. Haney
Corporation Counsel
Carmel, IN

Roger Horner
City Attorney
Brentwood, TN

Rose Humway-Warmuth
City Solicitor
Wheeling, WV

Monica Joiner
City Attorney
Jackson, MS

Stephen Kemp
Former City Attorney
Peoria, AZ

Art Pertile
City Attorney
Stafford, TX

Susan L. Segal
City Attorney
Minneapolis, MN

IMLA
THE MUNICIPAL LAWYER MAGAZINE



SPECIAL TECHNOLOGY ISSUE

PUBLIC SAFETY TECHNOLOGIES: THE FOURTH AMENDMENT BALANCING ACT

By Gary W. Schons, Best Best & Krieger, San Diego, California

Technological innovation is providing law enforcement with ever-more powerful tools for pursuing suspects and accessing their personal data. Does this represent an advance in public safety—or an attack on Constitutional rights?

Page 6

A WEALTH OF INFORMATION: THE IMPORTANCE OF DATA SECURITY FOR LOCAL GOVERNMENTS

By Devin Chwastyk, McNees, Wallace and Nurick, Harrisburg, Pennsylvania

Local governments receive and store terabytes of sensitive personal information about their constituents. If hacked, this data can be exploited to steal identities and cause unimaginable mayhem—and municipalities can be held liable.

Page 14

THE GOOD, (POTENTIALLY) BAD, AND (AVOIDING) THE UGLY: THE BENEFITS, CHALLENGES, AND OPPORTUNITIES DRIVERLESS VEHICLES OFFER TO MUNICIPALITIES

By Gregory Rodriquez, Best Best & Krieger, Washington DC

Autonomous vehicles are on the way. They will have a significant impact on localities, from revenues to land use to employment and far beyond. Municipalities need to be planning now for this for this new environment.

Page 18

DEPARTMENTS

17 AMICUS CORNER
Recent Qualified Immunity Cases
By Amanda Kellar, IMLA Associate General Counsel and Director of Legal Advocacy

22 FEDERAL
The FDA's First E-Cigarette Regulation
By Caitlin Cutchin, IMLA Associate Counsel

23 SECOND LOOK
Objecting to Requests for Production
By Pete Haskel, Executive Assistant City Attorney, Dallas, Texas

25 INSIDE CANADA
Cases of Interest
By Monica Ciriello, Ontario 2015

26 IMLA
Board of Directors Election

30 LISTSERV
The First Amendment and the Right to Toss Pizzas
By Brad Cunningham, Municipal Attorney, Lexington South Carolina

STAFF

EXECUTIVE EDITOR
Charles W. Thompson, Jr.

EDITOR
Erich R. Eiselt

EDITORIAL STAFF
Caitlin Cutchin

ART DIRECTION & PRODUCTION
Trujillo Design

Views appearing in Municipal Lawyer are those of the author. Publication of articles in this magazine does not reflect a direct or implied endorsement of an author's views. © Copyright 2016 by the International Municipal Lawyers Association (IMLA). All rights reserved. IMLA is a non-profit professional association of municipal lawyers from across the United States and Canada. It offers its members continuing legal education courses, research services, litigation assistance on amicus briefs and an information-sharing network in the field of municipal law. Municipal Lawyer is IMLA's membership magazine. It is published bi-monthly. Views expressed by authors and contributors are not necessarily the views of IMLA. For membership information contact: IMLA, 7910 Woodmont Avenue, Suite 1440, Bethesda, MD 20814, phone: (202) 466-5424, or e-mail: info@imla.org. Contributions of articles are welcome. Municipal Lawyer reserves the right to refuse or edit manuscripts submitted for publication.

EDITOR'S NOTE:

IMLA
THE MUNICIPAL LAWYER MAGAZINE

On May 19, 2016 the New York Civil Liberties Union brought suit against the New York City Police Department, demanding production of records about the NYPD's use of "Stingray." Deployed by more than 60 law enforcement entities nationwide, Stingray is a faux cell tower, capable of being utilized virtually anywhere. As one commentator describes it, Stingray calls out "Marco" and all cell phones in the area reply "Polo." Stingray then locates, identifies and monitors nearby phones, enabling the "good guys" to track the "bad guys." But, the ACLU argues, Stingray also captures data from countless other people who have no reason to be surveilled.

In the wake of tragedies like the Orlando Pulse attack, pressures will mount to employ ever-more intrusive surveillance techniques. Our timely lead article, "Public Safety Technologies" by Gary Schons of Best, Best & Krieger, discusses the Fourth Amendment complexities presented by Stingray and a spectrum of new law enforcement tools.

We examine other technologies as well. In "A Wealth of Information," Devin Chwastyk of McNees, Wallace and Nurick discusses the daunting challenges faced by municipalities in protecting the sensitive personal data entrusted to them against attacks by increasingly sophisticated hackers. And in "The Good, the Bad and the Ugly," BB&K's Greg Rodriguez takes a first look at yet another technological tsunami headed directly at local governments—driverless cars, which will upend traditional transportation models.

In our other departments, we welcome IMLA's newest lawyer, Caitlin Cutchin, who assesses the FDA's first E-cigarette regulation in "Federal." Pete Haskel instructs in the fine art of deflecting production requests in "Second Look." Cases of Interest are profiled by Monica Ciriello in "Inside Canada," and IMLA's Amanda Kellar spotlights the Supreme Court's recent qualified immunity decisions in "Amicus." Finally, our "ListServ" author, Brad Cunningham, considers the annoyance of unauthorized advertising on the front lawn in "The First Amendment and the Right to Toss Pizzas."

We hope you find this special Technology issue of ML instructive.

Best Regards-

Erich Eiselt

DO YOU HAVE AN ARTICLE FOR THE MUNICIPAL LAWYER?



IMLA members are involved in some of the most challenging and interesting legal issues of our time—First Amendment questions, environmental debates, law enforcement policies, taxation and finance, and many others.

Share your experience, insights and practice tips. Our readers include a wide range of government attorneys at the state, city, county and local level, many lawyers in private practice who specialize in municipal law, and law libraries across the country.

To Submit An Article, please contact the **Editor, Erich Eiselt, at eeiselt@imla.org** with a brief description of your topic.

Municipal Lawyer is published 6 times per year, and feature articles should be between 2,500 and 4,000 words in length.

Submitted articles are subject to review by IMLA staff, and IMLA reserves the right to edit articles (for style, clarity, length, etc.).

We look forward to hearing from you!

Questions? Please contact IMLA at info@imla.org.

EXECUTIVE DIRECTOR'S LETTER

Charles W. Thompson, Jr.
IMLA General Counsel and Executive Director

For IMLA another fiscal year has just come to a close. I am happy to report that our organization strengthened in many ways. First and foremost, we added new members while retaining our existing family of long-time IMLA stalwarts. We believe this growth was a response to our efforts to add value to the IMLA membership package. We saw our lower-priced Kitchen Sink distance learning program participation almost double, and our attendance at those events is now routinely reaching record levels. In Las Vegas, we had the best attendance at an annual conference in 10 years and our recent spring seminar in Washington DC also welcomed the most attendees in more than a decade. Our Section 1983 track was a resounding success, which we will be repeating. We are filing historic numbers of amicus briefs on behalf of IMLA municipalities. Members are contributing ever-more insightful articles to *Municipal Lawyer*. And the ListServ which we co-sponsor continues to provide a vital forum where local government attorneys freely share their advice and experiences in the pursuit of better public service.

All in all, IMLA has much to celebrate.

Frankly, none of our success would be possible without the dedicated staff with which IMLA is blessed. Anyone who has been to one of our conferences knows Trina Shropshire-Paschal. We could not operate our programming without her. Not only does Trina ensure CLE approval for our programs, keeping abreast of the requirements of 50 states and the various Law Societies in Canada, but she handles the registrations and issues that come up from time to time. Coupled with her professionalism, Trina brings genuine empathy to her job. I'm often amazed when a member comments on how Trina remembers a personal detail and asks about a family member's health or success.

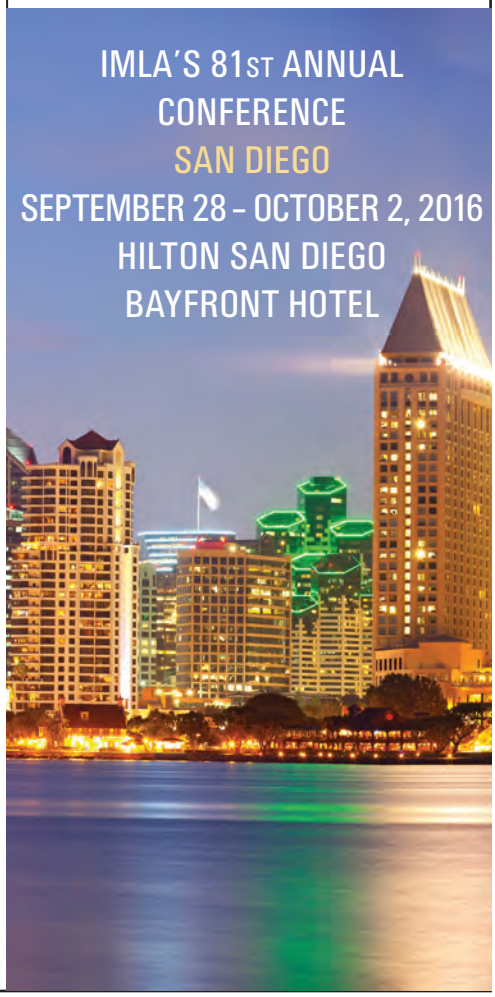
Jennifer and Julie Ruhe add enthusiasm and the competitiveness that each drew upon to be successful NCAA scholarship athletes. They are responsible for enhancing our conference experience by bringing "the app" to our devices, and continue to look at new technologies which will attract and serve our younger cohort of IMLA members. With the team's efforts we have seen memberships rise off of what we hope is a bottom and we have expanded our outreach via listservs and workgroups.

Our legal team has been doing amazing work over the past year. While we lost Tukie Falade to the GSA, we have gained our newest lawyer, Caitlin Cutchin, who has jumped right in to handle our distance learning while also doing research and writing for our members and our magazine. Erich Eiselt continues to lead *Municipal Lawyer*, offering excellent and timely articles—as evidenced by the focus on technology in this July-August *ML*, and has brought numerous leading-edge issues to our desks. Amanda Kellar heads our legal advocacy program while also heading up programming for our events. I'm not sure how she has the time. IMLA's legal advocacy program has flourished under her leadership, with more and more cases gaining our support. Each case requires review and evaluation before we send it to the committee and Amanda handles the task flawlessly and quickly.

This brings me to Veronica Kleffner, who as most of you know is planning to retire after the Niagara Conference next fall. For over 30 years, Veronica has been the rock that acts as the foundation for IMLA. I hope that all of our members, past and present, will come to the Niagara Conference to make it the biggest retirement party ever. I am not sure any organization has been blessed with a person as dedicated to its success. Each day Veronica brings professionalism and cheer to her role—and to the office, which like a benign virus spreads to us all. Even now she is overseeing IMLA's office move in September, from our long-time home in Bethesda to new offices in Rockville, Maryland.

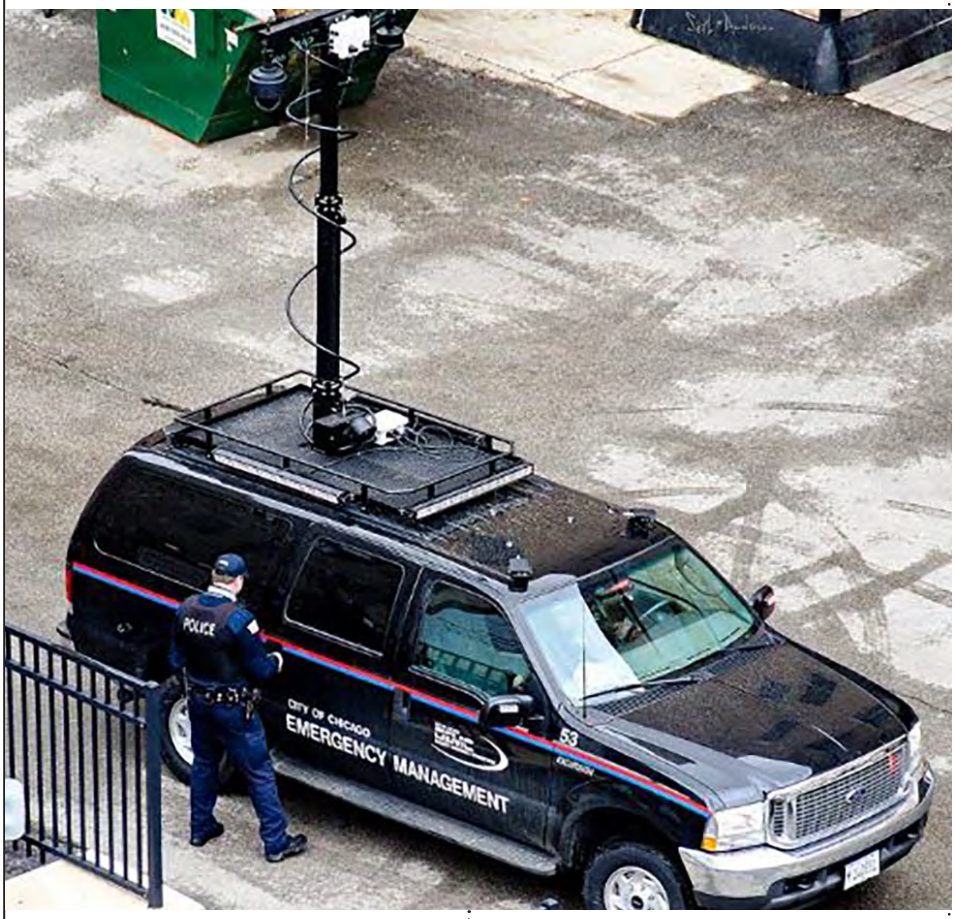
As IMLA end this fiscal year and looks to our future, the forecast is bright.

Let me conclude by getting up on my soapbox and urging you to work with IMLA to restore Home Rule to local governments and find ways to stop state and federal legislation designed to pull local option from locally elected leaders. Courts and legislatures alike seem to be working in tandem to erode local autonomy under the influence of special interests. IMLA is committed to supporting local autonomy for local governments and reducing their exposure to liability. To be successful we need to increase our membership and through the bonds of membership we can be a voice of reason. ML



Public Safety Technologies: Big Brother and the Fourth Amendment

By Gary W. Schons, Of Counsel, Best Best & Krieger, San Diego, California



Introduction-The Evolving Collision Between Law and Technology

Technological advancements in imaging, activity and sound detection, global positioning, data collection and mining, and biometrics are rapidly being adapted to law enforcement, enhancing public safety and facilitating criminal prosecutions. In parallel with these developments, the near-universal use of portable electronic devices is exposing ever more intimate personal details to monitoring and interception. At the crossroads of these technologies are concerns for privacy, civil liberties, the limits of government power, and the contours of ordered liberty in the 21st Century.

The principal restraint on governmental intrusions into "privacy" is the Fourth Amendment prohibition against unreasonable searches and seizures. Since *Katz*[1] a "search" has been recognized as a "prying into a private place," and what is "private" has been based on a person's subjective expectation of privacy. Recent technological advances have contorted the notion of "prying" and "privacy" at both ends of the spectrum. For example, armed with infrared detection devices, police can detect heat radiating from a home, indicating ongoing narcotics production. Is this "prying into a private place," or merely detecting heat emanating from a building?[2]

On the other hand, courts have generally found that police are entitled to search an arrestee's wallet or purse without a warrant. But what about searching a cellphone? Once this was permissible, but no longer.[3] As will be discussed, Fourth Amendment jurisprudence is in a constant race to keep up with advances in police-deployed technology, and some scholars believe that the Fourth Amendment alone cannot protect privacy from these new technologies.[4]

The Constitution is not the only bulwark against overreach. There are other sources for checks on technology-enabled police intrusions into "privacy". Restraints can originate in state legislatures.[5] Groups such as the ACLU have launched inquiries into law enforcement use of these technologies through Freedom of Information Act and Public Records Acts requests--with follow-on exposes driving changes in practices and procedures.[7] And local police agencies are responding to "civilian" oversight by developing policies which restrain use of advanced technologies.[8]

Supreme Court Responses at the Crossroads of Law Enforcement and Advanced Technologies

The Supreme Court has grappled with Fourth Amendment implications of technological advances in law enforcement for nearly a century. The progress of the law has been not been doctrinally consistent. The Court's 1928 *Olmstead* decision,[9] regarding telephone wiretaps, premised the determination of whether a "search" has occurred on the notion of physical trespass, and looked

to the place where the search was conducted. The 1967 *Katz* decision largely repudiated the "trespass" doctrine of *Olmstead* and instead focused on whether the search intruded into a place where a person had a reasonable subjective expectation of privacy.[10] However, over the last several decades, the Court reverted to sanctity for certain places, foremost the home,[11] and looked to the nature of the intrusion rather than the strict expectation of privacy, particularly when reviewing "sense enhancing" technology employed by law enforcement.

In *Kyllo* (the case previously mentioned involving thermal imaging to detect a marijuana grow operation inside a home), Justice Scalia wrote: "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search--at least where (as here) the technology in question is not in general use."[12] Thus, use of an "exotic" thermal imager might transgress the Fourth Amendment, while use of binoculars would not. Some scholars characterized this reasoning as

the "Walmart test,"[13] a particularly relevant construct when applied to commercially-available drones.[14]

Two fairly recent decisions by the Supreme Court illustrate the challenges in applying the Fourth Amendment to new technologies. *United States v. Jones*[15] questioned whether the police attaching a GPS tracking device to a vehicle, without a warrant, and use of the device to monitor the vehicle's movements on public streets for 28 days, constitutes a "search" under the Fourth Amendment. The GPS-derived data ultimately enabled police to locate a cache of 97 kilograms of cocaine and $850,000 and arrest Jones. He argued that the evidence must be suppressed. The government's argument was that under *Katz*, Jones had no reasonable expectation of privacy in the exterior of the vehicle or in locations the vehicle traveled on public roads, which made it visible to all. The government relied on one of the tenets of *Katz*: what a person knowingly exposes to the public, even in his own home or office, is not constitutionally protected.[16]

Writing for a unanimous Court, Justice Scalia impliedly rejected the government's *Katz*-based arguments, reverting to *Olmstead's* trespass-based understanding of the Fourth Amendment: "Here, the Court need not address the Government's contention that Jones had no 'reasonable expectation of privacy,' because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, the Court must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.' "[17]

What *Jones* seems to predict is that at least a majority of the Court would continue to look to *Katz's* reasonable expectation of privacy formulation in determining whether, in the context of emerging technologies, a Fourth Amendment search has occurred and whether that search is reasonable. (A search without a warrant is presumptively unreasonable, subject to certain specifically established and well delineated exceptions; while a search with a warrant is presumptively reasonable.)[18]

For at least 45 years, the Court told police they could conduct a warrantless search of a person arrested, including the "area into which he might reach," in order to protect material evidence or the officer's safety. This "search incident to arrest" doctrine meant that the police could search the personal effects of a person arrested, such as a purse, wallet, briefcase or backpack.[19]

When San Diego police arrested David Leon Riley for illegal possession of handguns, they seized a cellphone from his pocket, finding evidence connecting Riley to a gang-related murder. He was convicted, in part based on the evidence obtained from his cellphone.

Riley's challenge to this warrantless search eventually found its way to the Supreme Court in 2014. Riley's counsel argued that the cellphone was not like a wallet, purse, briefcase or backpack, and he warned that it could open up "every American's entire life to the police department, not just at the scene but later at the station house and downloaded into their computer forever."[20]

Writing for a unanimous Court, Chief Justice Roberts concluded that the rationale for the "search incident to arrest" doctrine--to protect officer safety or material evidence--could not justify the wholesale intrusion into the vast trove of a digital data on a cellphone without a warrant.[21] Officer safety was not implicated: "Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape."[22]

Nor did evidentiary value override Constitutional concerns. While the Chief Justice conceded that cell phone data could be vulnerable to remote wiping, and that an officer seizing a phone might not be able to search it before the phone locked and its data became encrypted, he emphasized that cell phones differ in both a quantitative and a qualitative sense from other objects in a person's pocket:

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.' The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. [23]

Riley is a stark example of advances in technology bending the arc of Fourth Amendment analysis. In truth, the search of a wallet, purse or briefcase could be just as intrusive and revealing as searching the digital information in a cellphone.[23] But the storage capacity of the cellphone and the uses to which it had been put in contemporary society simply overrode the law enforcement considerations which had shaped and sustained the "search incident to arrest" doctrine. This required a re-balancing of law enforcement and privacy interests and resulted in a requirement that police obtain a warrant before searching the digital data in a cellphone.

What seems to be emerging in the jurisprudence of the Supreme Court and lower federal and state courts[24] is a balancing of efficient law enforcement against the privacy rights of citizens, including movement, communications and identity, residences, and, importantly, personal effects.[25]

Cellphone searches are hardly the end of the story. Ever more innovative law enforcement technologies are emerging which will continue to challenge courts as they balance governmental interests against personal privacy rights:

Stingray—Locating Cellphones and Their Owners, in Real Time

Perhaps the most controversial surveillance technology now in the hands of the police is the Stingray, a cellular telephone surveillance device that identifies a cellphone's unique numeric identifier—its IMSI or ESN. Without any action by the phone's owner, cellphones regularly transmit

Continued on page 8



Gary Schons is a member of Best Best & Krieger's Public Policy and Ethics Compliance practice and counsels municipalities and private businesses who wish to promote public confidence in their processes. Prior to joining BB&K, he served as a deputy district attorney and senior advisor to the San Diego County District Attorney's Office, providing advice on public integrity issues to 300 deputy district attorneys in that office.

From 1976-2011, Gary was a member of the Criminal Division of the California Attorney General's Office, ultimately rising to head the Criminal Division in San Diego, where he supervised 75 attorneys who handled some 1,500 cases annually. He is a graduate of the University of San Diego School of Law, an avid cook, contributor of a dining column to the local paper and a golf and sailing enthusiast.

Public Safety Technologies Cont'd from page 7

data to cell sites or towers, including the phone's IMSI and the cell site code, which identifies the phone's location with great precision. The IMSI identifier imitates a cell site, collecting this data from all cellphones in the vicinity of the device.

If the police know a suspect's location, it can use the Stingray to determine the unique IMSI of the suspect's cellphone. This information can then be used to obtain call records for the phone or to obtain a wiretap for the phone itself. Conversely, if the police know the IMSI of the suspect's phone, it can then use the Stingray to locate of the phone (and suspect) with great precision, sometimes within seven feet. In certain configurations, the Stingray is capable of capturing the content of communications, such as voice calls and text messages.[26]

The Stingray is compact enough to be carried by hand (trade name "KingFish"), or can be mounted in a vehicle, a drone or an aircraft. It costs between $350,000 and $400,000.

Concerns over the use of the Stingray are many. Some of the 48 agencies in 20 states armed with the Stingray device are using it without a search warrant.[27] The Supreme Court has held that pen registers and "trap and trace" devices, which are older technology with functions analogous to those of the Stingray, are not subject to the Fourth Amendment warrant requirement because the user voluntarily conveys the numerical information—numbers dialed and calls received—to the telephone company.[28] However, a cellphone transmits IMSI and cell site information without any activity by the user. This may well serve to distinguish Stingray technology from traditional pen registers or "trap and trace" devices for Fourth Amendment purposes.

In November, 2015, Representative Jason Chaffetz (R-Utah) introduced the Cell-Site Simulator Act of 2015, also known as the Stingray Privacy Act. The bill would require state and local law enforcement to obtain a warrant before they could use Stingray devices, under threat of federal criminal prosecution.[29] The bill would also require law enforcement to disclose to a judge or magistrate how the Stingray technology operates, as opposed to some other surveillance tools like pen registers.[30] Five states—California, Minnesota, Utah, Virginia and Washington—have already passed laws requiring its officers to obtain a search warrant before using Stingray.[31]

Although police may be interested in only the particular cellphone and location of a particular suspect, the Stingray device sweeps up *all* cellphones in the vicinity when it is operating, thus capturing data from "innocent bystanders." There do not appear to be safeguards in place to protect this data. Additionally, law enforcement agencies have been secretive about the devices, citing confidentiality agreements with the manufacturer and the FBI.[32]

A recently California law addresses these concerns. Senate Bill 741 signed into law by Governor Jerry Brown in the fall of 2015 requires local agencies that operate cellular communications interception technology such as Stingray to maintain operational, administrative, technical, and physical safeguards to protect information gathered from unauthorized access or disclosure. The bill further requires that the local agency make its information usage and privacy policies available in writing to the public.[33]

Cellphone Tower Dumps—Searching the Haystack to Find the Needle

A "cellphone tower dump" is a process where law enforcement seeks information sent from cellphones to a cellphone tower. As previously noted, cellphone towers enable GPS in cellphones and allow phones to make and receive calls. Cellphones constantly search for a tower to connect to, and relay information even when not in use. That data is saved by the cellphone company for years and can include location information, call history, sent texts and even search terms typed into phone browsers.[34]

Department of Justice attorneys apply for court orders authorizing "dumps" under the Electronic Communications Privacy Act of 1986.[35] This requires a showing of relevance to an ongoing investigation, but not probable cause as required for a search warrant. Some scholars have argued that this information is entitled to Fourth Amendment protection which should require a showing of a probable cause and be released only pursuant to a search warrant.[37] So far, no U.S. court has adopted this argument, although a Canadian court has.[38] Law enforcement routinely seek thousands of these "dumps" annually.[39]

The concern of civil rights and privacy advocates is that these "dumps" reveal vast amounts of data about innocent persons, unrelated to any particular investigation. There is no accounting for how this "excess" data is handled.

In Canada, two of the nation's biggest telecommunications companies brought suit in an Ontario court to halt the practice, arguing that sweeping "tower dumps" violate the Charter of Rights and Freedoms.[40] On January 14, 2016 the judge ruled there was a breach of the Charter in "tower dump" production orders that required the two telecommunications companies to provide to police the personal information of about 40,000 users. The judge found that the disclosure of the personal information required went "far beyond what was reasonably necessary to gather evidence concerning the commission of the crimes under investigation."[41]



Range -R Radar in use

Range-R Radar—"Seeing" Suspects Through Brick Walls

Range –R radar is a handheld (10" x 4") Doppler radar device capable of penetrating most common types of building walls, ceilings and floors. While it does not provide an image, it is capable of detecting the presence and movement, even the breathing, of a person inside a building, up to 50 feet away. A unit costs about $6,000. The device was designed for U.S. military use in war zones like Afghanistan and Iraq;[42] however, its applications for domestic



Range -R Radar

law enforcement are evident. The device can be used to scan a building silently and quickly before officers enter, either to execute a search warrant or under exigent circumstances in which case a warrant is not required.[43] Its potentially life-saving utility for first responders and victims in fires, natural disasters, hostage, active shooter and other such critical events is clear. Given its low cost and utility, widespread deployment of Range-R Radar by law enforcement agencies is expected.[44]

The Fourth Amendment implications for Range-R seem clear. Whether shooting radar rays into a home would constitute a "trespass" might not need to be considered, because this is clearly "exotic" sense-enhancing technology that permits the police to "pry" or "peer" into a "private place"—a residence or office—which has the highest level of Fourth Amendment protection and for which there is an unassailable reasonable expectation of privacy. The *Kyllo* decision, previously discussed, has clear application to use of the Range-R device.[45]

In a recent 10th Circuit decision originating in Kansas,[46] the court had the opportunity to pass on the use of Range-R, which police used without a warrant before entering a residence to arrest a fugitive parolee. Because authorities had ample other evidence that the fugitive was inside the residence—old fashioned "gum shoe" work like noting heightened activity on the utility meter in the fugitive's name, knowing he was unemployed and likely at home during the day, and even footprints in the snow outside the residence—the court did not have to pass on the lawfulness of the use of the Range-R. However, the court did note the following:

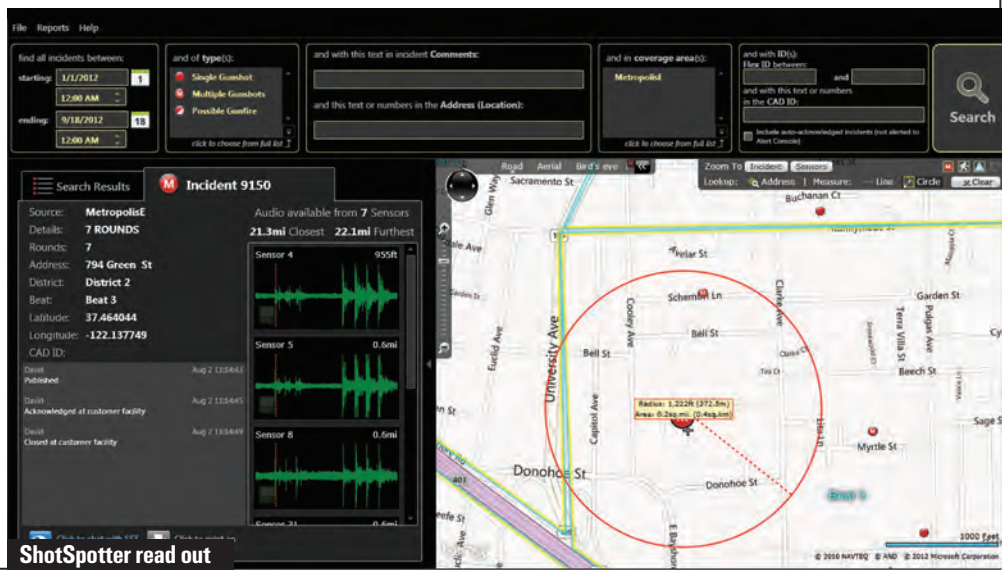
> Separately and as we alluded to earlier, the government brought with it a Doppler radar device capable of detecting from outside the home the presence of 'human breathing and movement within.' All this packed into a hand-held unit 'about 10 inches by 4 inches wide, 10 inches long.' The government admits that it used the radar before entering — and that the device registered someone's presence inside. It's obvious to us and everyone else in this case that the government's warrantless use of such a powerful tool to search inside homes poses grave Fourth Amendment questions. New technologies bring with them not only new opportunities for law enforcement to catch criminals but also new risks for abuse and new ways to invade constitutional rights. *See*, e.g., Kyllo v. United States, 533 U.S. 27, 33-35 (2001) (holding that using warrantless thermal imaging to show activity inside a home violated the Fourth Amendment). Unlawful searches can give rise not only to civil claims but may require the suppression of evidence in criminal proceedings. We have little doubt that the radar device deployed here will soon generate many questions for this court and others along both of these axes.[47]

It appears evident that the courts will find that use of the Range-R device, absent exigent circumstances, will require a search warrant. An officer applying for a warrant to search a residence or other structure can easily include a justification for authorization to use the Range-R device. In fact, this will likely become a commonplace feature of search warrant applications and orders.

ShotSpotter—Locating the Shooter in Real Time

ShotSpotter uses sophisticated triangulation technology combined with audio, acoustic, and possibly optical and other types of sensors to detect and convey the location of gunfire. According to the manufacturer, the system can pinpoint the location of shots fired to within 10 feet and notify police dispatchers in real time. Systems used in urban settings integrate geographic data so the display includes a map and address of each incident, helping first responders rapidly reach the scene of gunfire, thus increasing arrests rates, improving officer safety, securing witnesses and evidence, and enhancing investigations—as well as in the long run deterring

Continued on page 10



ShotSpotter read out

Public Safety Technologies Cont'd from page 9

gun crimes. Additional benefits include aiding investigators to find more forensic evidence to solve crimes and provide to prosecutors to strengthen court cases resulting in a higher conviction rate."

New York City has inaugurated a $1.5 million test system using more than 300 ShotSpotter sensors to cover 15 square miles.[48] This is a relatively benign, if not welcome technology.[49]

However, deployment of the technology might have unintended consequences. Civil rights and privacy advocates, while "not losing sleep over" the technology, have concerns about whether the systems will be able to detect voices.[50] In a case in Oakland, ShotSpotter captured the final words of a dying man who yelled out the gunman's name. This obviously assisted the police in locating the assailant and the prosecutor in convicting him.[51]

Automated License Plate Reader (ALPR)—Linking the Car to the Crime

Automated License Plate Reader (ALPR) technology uses fixed and mobile (in law enforcement vehicles) high-speed cameras which automatically take digital photographs of passing vehicles' license plates on public roads, using character recognition software to read the plates' numbers. Each photograph is time-, date- and GPS-location "stamped." In major metropolitan areas, these systems scan and store hundreds of thousands of license plates per week, which may be stored for years.

At virtually the same time the license plate is scanned, the system runs it against a list of known plates associated with suspected crimes, criminal investigations, outstanding warrants and AMBER alerts--a so-called "hot list." Law enforcement can also query the stored plate database in subsequent investigations. Of the over 70% of law enforcement agencies that employ ALPR, nearly all report a significant increase in crime interdiction as a direct result of the technology.[52]

There is no Fourth Amendment restraint on image capturing, scanning, storing, or cross-check features of the ALPR technology because it is capturing images in a public place where the police have a right to be and a vehicle owner has no reasonable expectation of privacy in his license plate.

Concerns about these systems have been raised by civil liberties groups and privacy advocates who express questions about the deployment of the system in certain communities, the capture of data that belongs to innocent persons, whether the technology allows for active surveillance and tracking of movement, and the length and depth of the retention of the data.[53]

To date, twelve states have passed legislation either restricting or regulating the operation of ALPR. These restrictions include limiting use to law enforcement, limiting data retention periods, imposing privacy restrictions, and requiring written policies governing system operations and data use and retention.[54]

Florida law creates a public records exemption for certain images and data obtained through the use of ALPR[55] In California, the ACLU has sued to obtain ALPR data from law enforcement under the state's Public Records Act. Although the ACLU lost in the lower courts on the grounds that that the "investigative records" exception to the California PRA covered all ALPR data; however, the California Supreme Court has granted review in the case.[56]

Biometrics—Making Anonymity Impossible

Biometrics refers to using human physiological characteristics as a form of identification or authentication and, in certain increasingly common applications, for access control.[57] It is estimated to be a $15 billion industry in the United States. Fingerprints are perhaps the original form of biometric identification, but biometric measures have now expanded to include DNA, facial recognition, scar and tattoo matching, palm print, iris scan and voice recognition. Even a person's gait can be quantified, measured and compared for identification purposes. Certain biometric measures produce highly reliable "matches," like DNA and fingerprints. Others, such as face recognition, produce "probables," chiefly of value in narrowing a set of suspects, or providing probable cause to pursue a "probable match."[58] Computing technology has vastly increased the power of biometric identification. As for example, computerized fingerprint and DNA databases can run millions of comparisons in seconds.[59] The power of biometrics has also been enhanced by improved imaging and location technologies.[60]

The FBI Biometric Center of Excellence serves as the principal law enforcement resource center and data repository, clearinghouse, and standard-setter for biometric data collection, input and applications. The Center has 29.3 million "searchable" photos and plans to expand this database to 52 million images.[61] State and local agencies contribute to and obtain assistance from the Center.[62] The FBI collects and uses data obtained only by legal means, e.g.. mugshots and fingerprints taken at post-arrest booking and evidence collected during a criminal investigation. It does not use "open sources" or social media as sources for data.[63] As part of its mission, the Center regularly accesses privacy concerns and issues Privacy Impact Assessments,[64] although this process has not been without its critics.[65]

The legality of these biometric collection, data retention, and comparison processes is clear. However, civil liberty and privacy advocates have voiced concerns over the standardless collection of biometric data, alleged indiscriminate expansion of these databases to include nearly every citizen, and the ability to make instantaneous matches, often without sufficient standards, clear rules or oversight-.[66] The *New York Times* reported on incidents in San Diego in which officers took photos of or obtained DNA samples by way of a buccal swab from individuals lawfully detained for minor offenses, and then ran the biometric data through the national database. At the time of the report the San Diego Police Department had no written policy to guide the actions of its officers. The story went on to report that over a 33-day period in January and February 2015, 26 San Diego County law enforcement agencies used facial recognition software to seek to identify individuals on more than 26,000 occasions.[67]

Clearly, these are serious concerns surrounding this expanding technology; concerns which apply to both governmental and private use of biometric identification. Only a handful of states have passed laws regulating biometric collection and sharing by state or local agencies--Arizona, Illinois, Louisiana,

Maine, Missouri, New Hampshire, Oregon, Texas and Washington[68] and currently only Illinois and Texas have laws addressing private collection of biometric data for commercial purposes.[69] While other states can be expected to respond, it will fall to local policy makers to adopt practices that serve the interests of transparency, accountability and privacy in the application of this technology.

Threat Scoring ("Beware" Software)—Combining Criminal Markers

In January 2016 the *Washington Post* published a report on a new technological application coming into the hands of police departments--"Beware" software--which searches billions of data points, including arrest records, property records, commercial databases, Web data and individuals' social-media postings to arrive a "threat" score. The technology can be applied to a vehicle license plate number, an address or an area of a community. The *Post* article centered on the Fresno Police Department's deployment of Beware in its Real Time Crime Center, which brings together a number of technologies to follow incidents as they unfold. Such centers also exist in New York, Houston and Seattle.[70]

Police hail the technology as being able to provide real time information on suspects and persons of interest even as the police response is in motion. An example, cited in the *Post* article, concerned officers responding to a 911 call about a man threatening his ex-girlfriend. While patrol officers were in route, a police operator ran the individual through the Beware system and determined he had a firearm conviction and gang association,[71] so out of an abundance of caution, police called in a negotiator. But, police could employ this technology outside responding to an emerging situations, such as applying it to protesters or members of a group of concern to law enforcement.[72]

The legality of using Beware technology is not seriously in doubt. Nevertheless, the reaction of the privacy and civil liberties community was, to borrow an expression, fast and furious[73] as was that of the Fresno City Council when a councilmember "earned" a moderate threat score based on his residential address being connected to criminal activity prior to his moving there. The potential for abuse and error and the lack of "civilian" oversight and well-crafted policies are the foremost concerns. State and local legislative bodies may act to regulate or guide the use of this technology in coming months.

The ACLU has identified eight problems with the use of Beware technology:

- Scoring Americans in secret;
- Inaccurate data;
- Questionable effectiveness;
- Unfairness and bias;
- Potentially dangerous results;
- Unjustified government intrusion;
- First Amendment concerns;
- Mission creep. [74]

Conclusion

Some of the concerns expressed by the ACLU and the courts can be addressed, and perhaps ameliorated, through legislation, policies, "best practices," and refinements based on trial and error and experience. However, other concerns are inherent in the technology, requiring policy makers to balance the value of enhanced security against the new technology's potential for misuse.

For municipal lawyers advising law enforcement agencies and their cities, these technologies pose significant-but not insurmountable-challenges. First, the municipal lawyer needs to be aware of the technologies, their uses and capabilities, and existing legal restraints on their use, whether constitutional or statutory. Second, the municipal lawyer needs to be sensitive to the public policy implications of these technologies, including privacy, security, public safety and legal liability. Finally, the municipal lawyer needs to be a thought-leader in helping to design policy, protocols and best practices for the responsible deployment of these technologies.

Notes

1. Katz v. United States, 389 U.S. 347(1967).
2. Kyllo v. United States, 533 U.S. 27 (2001).
3. Riley v. California, 134 S. Ct. 2473 (2014).
4. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich L. Rev. 801, 838 (2004); Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 Minn. L. Rev. 1325 (2002); Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 Miss. L.J. 5 (2002).
5. For example, in 2015, the California enacted the Electronic Communications Privacy Act to prohibit law enforcement from compelling the production of electronic communication information or electronic device information without a search warrant or court order. (SB 178, adding Section 1546 et seq. to the California Penal Code.)
6. Joseph Goldstein, *New York Police are Using Covert Cellphone Trackers, Civil Liberties Group Says*, N.Y. Times, Feb. 11, 2016, http://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html?_r=0; Greg Moran, *Cell-Tracking 'Stingray' Device was Kept Secret*, San Diego Union Trib., Feb. 13, 2016, http://www.sandiegouniontribune.com/news/2016/feb/13/cell-tracker-nondisclosure/; Matthew Cagle, *Documents Reveal Anaheim, CA Has Surprisingly Robust Surveillance Arsenal for Small City*, ACLU (Jan. 27, 2016, 6:45 PM), https://www.aclu.org/blog/free-future/documents-reveal-anaheim-ca-has-surprisingly-robust-surveillance-arsenal-small-city.
7. See Jay Stanley, *Police Body-Mounted Cameras: With Right Policies in Place, A Win for All*, ACLU, (last updated March 2015), https://www.aclu.org/police-body-mounted-cameras-right-policies-place-win-all.
8. Olmstead v. United States, 277 U.S. 438 (1928).
9. Katz v. United States, 389 U.S. 438 (1967).
10. *Compare* United States v. Knotts, 460 U.S. 276 (1983) (use of "beeper" to track drug manufacturing products in a vehicle did not require a warrant), *with* Kyllo v. United States, 533 U.S. 27 (2001)(use of thermal imaging to detect heat emanating from a residential marijuana grow operation required a warrant).

Continued on page 12

Public Safety Technologies Cont'd from page 11

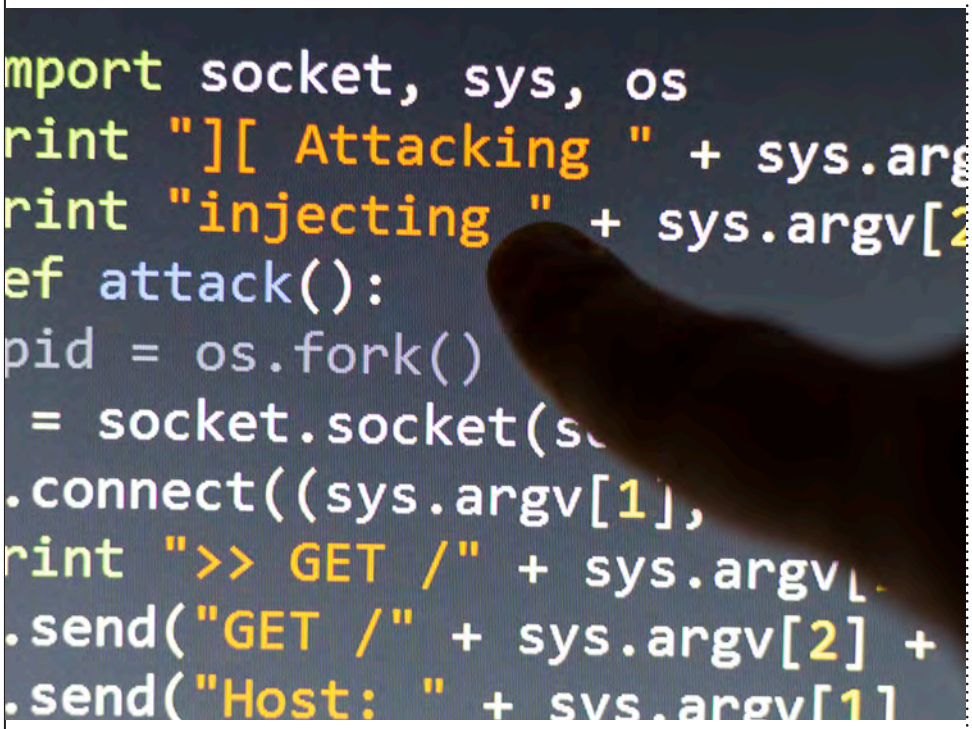
11. Kyllo v. United States 533 U.S. at 39.
12. Christopher Slobgrin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo's *Rules Governing Technological Surveillance*, 86 Minn. L. Rev. 1393 (2002).
13. The Supreme Court has twice held that the Fourth Amendment does not require police to obtain a warrant before observing what any other member of the public could with the naked eye, even when that observation takes place in the public airspace. (Florida v. Riley, 488 U.S. 445 (1989) (police helicopter); California v. Ciraolo, 476 U.S. 207 (1986) (police in a fixed-wing airplane.) *See also* Dow Chemical Co. v. United States, 476 U.S. 277 (1986)(EPA's use of a commercial aerial photographer using a precision aerial camera to photograph a chemical plant did not violate the Fourth Amendment).
14. The Supreme Court has twice held that the Fourth Amendment does not require police to obtain a warrant before observing what any other member of the public could with the naked eye, even when that observation takes place in the public airspace. (See, Florida v. Riley, 488 U.S. 445 (1989) (police helicopter); California v. Ciraolo , 476 U.S. 207 (police in a fixed-winged airplane). *See also* Dow Chemical Co. v. United States, 476 U.S. 227 (1986) (EPA's use of a commercial aerial photographer using a precision aerial camera to photograph a chemical plant did not violate the Fourth Amendment).
15. 132 S.Ct. 945 (2012).
16. Katz, 389 U.S. at 351.
17. *Id.*
18. *See* Chimel v. California, 395 S.Ct. 752, 763 (1969).
19. Erin Fuchs, *Supreme Court Hears Case That Could Open Up 'Every American's Life to the Police Department*,' Business Insider (April 29, 2014), http://www.businessinsider.com/supreme-court-hears-riley-v-california-2014-4.
20. Riley v. California, 134 S. Ct. 2473 (2014).
21. The Chief Justice could not have anticipated the recent furor and legal proceedings over the FBI's effort to gain access to the San Bernardino terrorist's Apple IPhone, which locked after he was shot and killed and which cannot be opened without Apple creating software to bypass its own security technology. Apple's locking and encryption technology may well have changed this calculus while the ink is barely dry on the *Riley* decision. *See*, Rosenthal, *Why Apple's CEO and the FBI are Fighting over Your Phone*, Mother Jones (Feb. 17, 2016 6:44 PM), http://www.motherjones.com/politics/2016/02/apple-ceo-tim-cook-san-bernardino-iphone.
22. Riley, 134 S. Ct. at 2473.
23. *Compare*, United States v. Vargas, F.Supp.2d (E.D. Ore. 2014), (No. CR-13-6025-EFS) (pole mounted camera that surveilled a front yard for six weeks without a warrant violated the Fourth Amendment), *with* United States v. Houston, 813 F.3d. 282 (6th Cir. 2016) (pole mounted camera that surveilled a rural property for 10 weeks did not require a warrant, Jones distinguished).
24. *See, e.g.*, Paul Larkin, *The Fourth Amendment and New Technologies*, Heritage Foundation Legal Memorandum #102 (Sept. 19, 2013), http://www.heritage.org/research/reports/2013/09/the-fourth-amendment-and-new-technologies.
25. Federal policy, adopted in October 2015, prohibits such use of the Stingray, effectively a wire intercept. *See*, U.S. Dep't of Justice, Use of Cell-Site Simulator Technology (2014), *available at* http://www.justice.gov/opa/file/767321/download.
26. With limited exceptions, USDOJ policy requires that federal officers obtain a search warrant based on a showing of probable cause before using the Stingray. *Id.* California's Electronic Communications Privacy Act requires officers to obtain a search warrant to use a Stingray device. *See supra* note 5. However, The New York Times reported that the NYPD obtains court authorization for use of the Stingray on the lesser standard applicable to pen register devices, namely, that information likely to be obtained from the device is "relevant" to an ongoing criminal investigation. N.Y. Crim. Pro. Law, Art.705 § 705.10; *see also* 18 U.S.C. § 206. *See* Goldstein *supra* note 6.
27. Smith v. Maryland, 442 U.S. 735, 744(1979).
28. Kim Zetter, *New Bill Would Force Cops to get Stingray Warrants*, Wired (November 3, 2015, 3:27 PM), http://www.wired.com/2015/11/new-bill-would-force-cops-to-get-warrants-before-spying-with-stingrays/new-bill- would-force-cops-to-get-warrants-before-spying-with-stingrays/. 29. There are documented cases in which police have obtained court orders to authorize trapping cellular telephone information without advising the judge that the Stingray technology would be employed. Nathan Freed Wessler, *New Evidence Shows Milwaukee Police Hide Stingray Usage from Courts and Defense*, ACLU (Jan. 25, 2016, 1:15 PM) https://www.aclu.org/blog/free-future/new-evidence-shows-milwaukee-police-hide-stingray-usage-courts-and- defense.
30. California (SB 178 (2015)); Minnesota (SF 2466 (2014)); Utah (1HB128 (2014)); Virginia (HB 1408 (2015); Washington (HB 1440 (2015))
31. *See* Larry Greenemeier, *What is the Big Secret Surrounding Stingray Surveillance,* Scientific American, June 25, 2015 http://www.scientificamerican.com/article/what-is-the-big-secret-surrounding-stingray-surveillance/ . Examples have been documented in New York, San Diego, and Anaheim, California. *See supra* note 5.
32. Jeff McDonald, *Police Slow to Post 'Stingray' Policies*, San Diego Union Trib., Jan. 13, 2016 http://www.sandiegouniontribune.com/news/2016/jan/13/stingray-policies/.
33. John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA Today, http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/ (last visited June 7, 2016).
34. Pub. L. No. 99-509, 100 Stat. 1848 (1986). U.S. Dep't of Justice, Law Enforcement Telephone Investigations Resource Guide 7 (updated Mar. 10, 2010), *available at* http://cryptome.org/isp-spy/le-tel-spy.pdf.
35. California Electronic Communications Privacy Act, Cal. Penal Code, §§ 1546 et seq. (SB 178 (2015).
36. Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 J. Const. L. 1 (2013).
37. *Id.*

38. Katie Hass, *Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions*, ACLU (March 27, 2014, 11:58 AM), https://www.aclu.org/blog/cell-tower-dumps-another-surveillance-technique-another-set-unanswered-questions.
38. Mike Crawley, *Police Sweeps of Cellphone Data In 'Tower Dumps' Face Charter Challenge*, CBC News (Jan 13, 2016, 5:52 PM), http://www.huffingtonpost.ca/2016/01/14/police-sweeps-of-cellphone-data-in-tower-dumps-face-charter- challenge_n_8975432.html.
40. *Ontario Court Rules Police Orders Breached Cellphone User's Charter Rights*, The Globe and Mail (Jan. 14, 2016), http://www.theglobeandmail.com/report-on-business/industry-news/the-law-page/court-sides-with-telecoms- in-landmark-cellphone-privacy-case/article28180968/
41. *See Police Use High-tech Radar to Warrantlessly Monitor People Inside Their Homes*, Police State USA (Jan. 21, 2015), http://www.policestateusa.com/2015/range-r-radar/.
42. "Exigent circumstances," which would justify the warrantless entry of a home or other structure are present as a matter of law "(1) to engage in hot pursuit of a fleeing felon; (2) to prevent the imminent destruction of evidence; (3) to prevent a suspect from escaping; and (4) to prevent imminent harm to police or third parties." United States v.
Washington, 573 F.2d 279, 286-287 (6th Cir. 2009); accord, United States v Daws, 711 F.3d 725 (6th Cir. 2013).). And, in *Brigham City v. Stuart*, 547 U.S. 398 (2006), the United States Supreme Court found that exigent circumstances include the need to assist an injured occupant or prevent injury.
43. It has been reported that as of early 2015, more than 50 law enforcement agencies, including the FBI and U.S.Marshals Service, had deployed the device. Erik von Ancken, *New Police Device 'Sees' Through Walls*, Click Orlando (Jan. 20, 2015, 6:58 PM), http://www.clickorlando.com/news/new-police-device-sees-through-walls.
44. Also applicable is the U.S. Supreme Court's decision in *Florida v. Jardines*, 569 U.S. 1 (2013), in which case the Court held that police use of a trained detection dog to sniff narcotics on the front porch of a private home constituted a "search' under the Fourth Amendment, and therefore required a search warrant.
45. United States v. Denson, 775 F.3d 1214 (10th Cir. 2014).
46. *Id.*
47. Christopher Moraff, *Shotspotter Coming to a Streetlight Near You?*, Next City (Oct. 7, 2015), https://nextcity.org/daily/entry/shotspotter-installed-in-city-streetlights-ge.
48. Tammerlin Drummond, *How Valuable a Policing Tool is Spotspotter?*, East Bay Times, (May 6, 2015, 3:35 PM) http://www.eastbaytimes.com/breaking-news/ci_28063140/drummond-how-valuable-policing-tool-is-shotspotter, reporting that Oakland had a 26 percent reduction in gunfire per square mile since 2013.
49. Jay Stanley, *Shotspotter CEO Answers Questions on Gunshot Detectors in Cities*, ACLU, (May 5, 2015), https://www.aclu.org/blog/free-future/shotspotter-ceo-answers-questions-gunshot-detectors-cities.
50. Paul T. Rosynsky, *Man's Dying Words Help Convict Oakland Killer*, Oakland Tribune, Oct. 26, 2010, http://www.insidebayarea.com/oaklandtribune/localnews/ci_16439539?source=rss.
51. David J. Roberts and Meghann Casanova, Automated License Plate Recognition Systems: Policy and Operational Guidance for Law Enforcement, International Assoc. of Chiefs of Police, March. 2012, *available at* https://www.ncjrs.gov/pdffiles1/nij/grants/239604.pdf ; Tod Newcombe, *States Start Restricting Police License Plate Readers*, Governing, August 12, 2015, http://www.governing.com/columns/tech-talk/gov-automated-license-plate-readers-police.html.
52. *You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements*, ACLU, https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf (last visited June 9, 2016); Mariko Hirose, *Documents Uncover NYPD's Vast License Plate reader Database*, (Jan. 25, 2016, 10:30 AM) https://www.aclu.org/blog/free-future/documents-uncover-nypds-vast-license-plate-reader-database.
53. National Conference of State Legislatures, *ALPR: State Statutes Regulating Their Use*, Feb. 18. 2016, http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of- automated-license-plade-readers-alpr-or-alpr-data.aspx.
54. Fla. Stat. 316.0777 (2014).
55. ACLU Found. of S. California v. Super. Court (City and County of Los Angeles), S227106 http://appellatecases.courtinfo.ca.gov/search/case/dockets.cfm?dist=0&doc_id=2111782&doc_no=S227106.
56. For example, VISA and MasterCard are rolling out facial and fingerprint biometric authentication for security and access control for charging and payments. *See* Find Biometrics Global Identify Management, *MWC 2016: A Personal Tour of MasterCard's Biometrics* (Feb. 26, 2016), http://findbiometrics.com/mwc-2016-a-personal-tour-of- mastercard-biometrics-302267/.
57. *See* FBI Biometric Center of Excellence, *Fingerprints and Other Biometrics*, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics [hereinafter FBI Biometrics] (last visited June 9, 2016).
58. *See* Jennifer Lynch, *FBI Combines Civil and Criminal Fingerprints into One Fully Searchable Database*, Electronic Frontier Foundation (Sept. 15, 2015), https://www.eff.org/deeplinks/2015/09/little-fanfare-fbi-ramps-biometrics-programs-yet- again-part-1.
59. *See* William Abernathy et. al., *Biometrics: Who's Watching You*, Electronic Frontier Foundation (Sept. 2003), https://www.eff.org/wp/biometrics-whos-watching-you.
60. Jennifer Lynch, *FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, Electronic Frontier Foundation (April 14, 2014), https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face- recognition-database-next-year The FBI claims an 80% "match" rate for its facial recognition technology.
61. *See* FBI Biometrics *supra* note 57.
62. FBI Biometric Center of Excellence, *FBI Biometric Specifications (BioSpecs)*, https://www.fbibiospecs.cjis.gov/ (last visited June 9, 2016).
63. *See, e.g.*, *Privacy Impact Assessment for eGuardian System*, Fed. Bureau of Investigation (Jan. 4, 2013), https://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat.
64. *See* Adam Wisnieski, *The FBI is Watching You*, The Crime Report (Oct. 27, 2014) http://www.thecrimereport.org/news/inside- criminal-justice/2014-10-the-fbi-is-watching-you.

Continued on page 21

A Wealth of Information: The Importance of Data Security for Local Governments

By Devin Chwastyck, McNees, Wallace and Nurick, Harrisburg, Pennsylvania



In February 2016, a computer hacker sent an e-mail infected with a "ransomware virus" to an employee of the town of Medfield, Massachusetts. When the e-mail was opened, the virus spread throughout the town's computer network, locking up the servers and preventing officials from accessing municipal data. A week of consultation with law enforcement and information technology experts brought only fruitless efforts to unlock the files. The town's officials then gave in to the hacker's demand: they paid a ransom by transferring funds (in the form of bitcoins, an electronic currency) per the intruder's instructions.

The town was lucky. In exchange for the payment, the hacker provided a software key that allowed the town to regain access to its files. Upon inspection, the files were untouched, and no data had been stolen.

Municipalities Are Especially At Risk Of Data Breaches

It is no surprise that a municipality would make an attractive target for a malicious hacker looking to steal or ransom valuable information. For taxation and other purposes, local governments routinely collect and maintain files of private and confidential information about their residents. Personally-identifiable information abounds in public records, including names, addresses, dates of birth, and Social Security numbers. When left exposed and taken up into the wrong hands, that information can be used to perpetuate identity theft and other fraudulent activity.

Modern technology utilized by local governments also provides opportunities for hackers. The federal government has warned that utilities are a major target for both independent and foreign, state-sponsored intruders. Smart city platforms, traffic control devices, and emergency notification networks offer hackers openings to steal data or disrupt infrastructure and daily life in cities and towns.

But it is not only sophisticated computer hackers that pose risks for local governments. Most data exposure events happen not due to theft, but through ordinary loss or inadvertent exposure. In early 2016, a local tax agency in Breckville, Ohio announced that it had lost a data storage device containing the names, addresses, Social Security numbers, and dates of birth of more than 50,000 taxpayers. Similarly, the county government in Dallas, Texas notified residents in December 2015 that a security flaw had left the same types of information, belonging to tens of thousands of those residents, exposed on a public website for more than a decade.

Though not appearing as malicious as intrusions by hackers, these sort of data breaches nonetheless result in significant costs and consequences for municipalities. Even if information has not been stolen or used for fraud, its mere exposure triggers legal obligations and liabilities for local governments.

Legal Obligations For Protection Of Data

The primary legal obligation arising when a data breach occurs is the duty to notify all individuals whose records were exposed. While there is no federal law addressing data breaches, forty-seven states and the District of Columbia now have laws requiring data security breach notifications.[1]

In most states, the requirement to notify affected persons that their information has been exposed to unauthorized third parties extends to any entity that maintains, stores, or manages computerized data, including municipalities and political subdivisions.[2]

Personal information is most commonly defined to include an individual's name, in combination with any of the following: (1) Social Security number; (2) driver's license or state identification number; or, (3) financial account information, such as credit or debit card or bank account numbers, in combination with a security code or password.[3] Increasingly, that definition has been broadened to encompass other categories, including medical information[4] and biometric data[5] such as fingerprints and retina images.[6]

Generally, an entity storing computerized data is required by these state data breach notification laws to provide notice whenever it discovers or reasonably believes that unauthorized persons have accessed and acquired unencrypted files containing un-redacted personal information.[7]

In a few states, however, notification is required as soon as unauthorized access is detected, regardless of whether there is any proof that the information has been acquired by third parties.[8] Some state laws, however, provide that an entity need not provide notice if it can determine that there is no reasonable likelihood that the information

has been or will be misused.

Responding to a data breach therefore requires careful scrutiny of the notification requirements of multiple states, as each state's law governs the notification that must be provided to its residents. A breach of a county government in New York, for example, may expose information of county employees who commute from New Jersey. Privacy attorneys must ensure that various divergent requirements of state law are met, which may require distribution of multiple notices. Some states require not only that notice of the breach be sent to the individuals affected, but also to the state attorney general's office, consumer affairs division, or police agencies.

The Costs Of Data Exposure

While notification alone can be an expensive endeavor when thousands of records are involved, the expense of mailing notices is not the only direct cost of a data breach. A municipality that is hacked will need to pay IT experts to investigate, repair, and secure the breached data network, and likely need to pay attorney's fees for outside privacy counsel. While not legally required, many entities that suffer a breach make offers to provide identity theft monitoring and protection to the affected persons, which also can be expensive.[9]

Several reliable studies have examined these costs of responding to a data breach. Those findings demonstrate that the average cost for a public sector entity to respond to a data breach is approximately $80 per individual record exposed.

Let's revisit the example of Dallas County, Texas. Because of an error, files containing the names and Social Security numbers of tens of thousands of residents were left unencrypted, un-redacted, and open to public exposure. Assuming a cost of $80 per record, a breach of this extent will almost certainly cost a municipality millions of dollars to respond to the incident, remediate, and secure again its computer systems. Those costs increase exponentially if more records are involved.

And these substantial costs are incurred even before any litigation commences. When a data breach becomes public, the entity that failed to secure personal information often finds itself the target of class action lawsuits.[10] A town then might find itself defending allegations that it negligently failed to secure the information that it collected and maintained about its taxpayers.

In 2013, vulnerabilities plagued the network of the Maricopa County, Arizona, Community College District, which held Social Security numbers and other data belonging to nearly 2.5 million former students, employees, and vendors. That information was available for access by unauthorized third parties for several years, while the District failed to take any steps to improve its data security. Importantly, there were never any reports of actual identity theft or fraud tied to the breach.

Nonetheless, the District was hit with multiple class action lawsuits. At last count, administrators estimated that the District had paid more than $20 million in notifications, legal settlements, credit monitoring costs, and network security upgrades.

For public entities battling tight budgets, such costs of responding to a data breach could be crippling. And the impact of a breach is not just financial. Victims of identity theft spend an average of nearly 100 hours working to resolve the situation. Just as a hacked business must regain credibility with its customers, a local government that fails to protect the information provided by its residents will need to work hard to rebuild public trust and confidence in the wake of a breach.

Steps To Limit The Risk Of Data Breaches

Municipalities therefore must proactively seek to limit the risks of data breaches and the ensuing liabilities. Privacy lawyers and IT professionals agree that data breaches are nearly inevitable, and so entities must seek to be "compromise ready." This can be accomplished through training and education, security assessments and IT support, strong data security policies, appropriate breach response plans, and attention to insurance and indemnification issues.

Training and education of employees about the importance of data security and risks of data breaches must be increased in the public arena. A 2015 poll of local government employees revealed that almost half were unaware of their employer's IT security practices. By comparison, in the private sector, a survey by the New York Stock Exchange found that data security is addressed at most or all board meetings of publicly-traded companies. Employees must be instructed about the importance of strong passwords, and systems should require the same. Training employees to recognize "phishing" attempts and avoid opening emails or attachments from unfamiliar addresses will greatly reduce the opportunity for hackers to introduce malware or ransomware into government computer networks. For attorneys and IT staff, organizations for privacy professionals offer training and certification with regard to and federal privacy laws and industry best practices.

While IT costs can burden already strained municipal budgets, the importance of devoting adequate funds to internal IT staff and resources, together with appropriate third party vendors, cannot be overstated. Most hackers gain access to computer systems when inadequate attention is devoted to their upkeep. Internal IT staff must have the resources to ensure that anti-virus, anti-spyware, and monitoring software, along with and software patches and firmware updates are kept current. Outside vendors, meanwhile, can conduct independent penetration testing and probe the network for files that may inadvertently have been left unencrypted and accessible to the public.

The process of creating a data security policy can force an entity to confront the categories and amount of personal information that they are collecting and storing. The best way to avoid a breach that exposes such information is not to collect it at all, or to retain it only so long as necessary to serve a necessary purpose.

A properly-devised data security policy will be written, will be disseminated throughout the organization so that all employees are familiar with the policy, and will address certain key topics.

First, the policy should designate an employee to coordinate the organization's data security efforts, including implementation, training, and testing of the policy.

Second, the policy should limit the categories of personal information that will be collected, limit access to those records to the employees whose duties require such access, and require that such records be destroyed or deleted at the earliest opportunity (consistent with organizational needs and legal retention

Continued on page 16



Devin Chwastyk, CIPP/US, is chair of the Privacy & Data Security group at McNees Wallace & Nurick. He counsels the firm's clients with regard to privacy issues, including the development of data security policies and data breach response plans. He also assists clients in responding to data breaches, including in rectifying, investigating, and reporting hacking and other data exposure events.

A Wealth of Information Cont'd from page 15

requirements). The policy should include or reference a document retention policy that addresses the full gamut of records the organization may collect or create. The data security policy must also provide for levels of disciplinary measures to be imposed if employees break or ignore the mandates addressing information security.

Third, the policy should address technical requirements, such as the updating and patching of software and firewalls, strong password requirements, and mandatory use of anti-virus protections. It is also crucial to prohibit the transfer of unencrypted personal information by e-mail or to portable devices, including storage media. All of the requirements regarding the security of electronically-stored personal information apply equally to the storage of such information in paper records and files.[11]

In addition to a data security policy, local governments should have in place a data breach response plan. When a breach occurs, the plan will designate the key decision makers, including public officials and legal and IT staff members. The plan should refer these leaders to a preselected forensics firm that can identify the scope of the compromise and repair the system without compromising digital evidence. And it will walk them through a decision tree that touches upon issues including contacting law enforcement, retaining outside counsel, determining notification obligations, documenting response steps, and addressing public relations. The breach response plan should require occasional drills to simulate a breach, with follow-up to refine the plan and for training purposes.

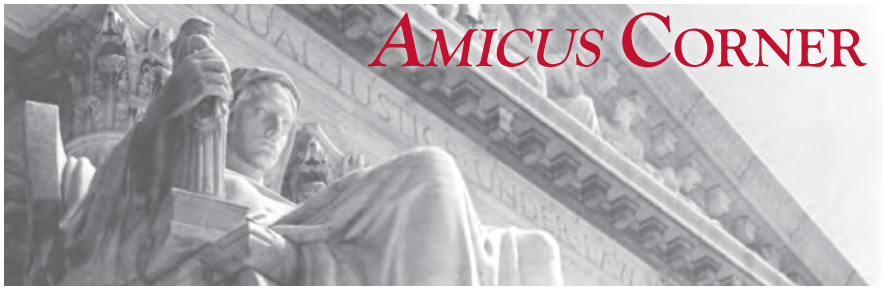
Insurance for data breaches should be a significant area of attention for municipal lawyers. It should be emphasized nearly all general commercial liability policies exclude coverage for data breaches. An insured must select requisite endorsements or separate policies for cyber-liability coverage. Coverage under an appropriate cyber-liability policy should include the costs of forensic analysis, repair of systems, data breach notifications, offers of credit monitoring, and, if necessary, legal defense of claims arising from a breach.

In addition to adequate insurance coverage, exposure also can be limited through inclusion of appropriate indemnification provisions in contracts with vendors. If any contractor is provided access to a municipality's physical office spaces, computer systems, or stored information, the contractor should be required to indemnify the municipality if their negligence (or intentional acts of their employees) results in any exposure of government data.

Herbert A. Simon, a Nobel laureate political and computer scientist, is known for his contributions in fields of study including artificial intelligence, organizational structures, and information processing. He wrote that a "wealth of information creates a poverty of attention and a need to allocate that attention efficiently ..."[12] For municipal governments, the wealth of personal information they must collect and maintain about their residents requires that substantial attention be devoted to the security of their computer networks and to preparation for the creeping inevitability of a data breach.

Notes

1. Only Alabama, New Mexico, and South Dakota have no breach notification law.
2. Some state breach notification laws limit the entities who must give notice to those "engaged in commerce" or "conducting business," or otherwise expressly do not include political subdivisions as subjects of the breach notification requirements: Arkansas; Colorado; Connecticut; Delaware; District of Columbia; Maine; Maryland; Michigan; Minnesota; Mississippi; Montana; Nebraska; New York; Rhode Island; Texas; Wyoming.
3. *See*, *e.g.*, Pennsylvania's Breach of Personal Information Notification Act, 73 PA. CONS. STAT. § 2302 (2016).
4. *See*, *e.g.*, FLA. STAT. § 501.171 (2016).
5. *See*, *e.g.*, IOWA CODE § 715C.1 (2016).
6. The increasingly expansive legal conception of personal information is expressed in the European Union's revised General Data Privacy Regulation, which will become effective in the spring of 2018. That regulation, which applies to companies that collect or process personal information of EU residents, extends the concept of personal data to encompass IP addresses, online identifiers, and nearly any other information that could be used to identify a person. *See* Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on The Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L 119/2).
7. *See*, *e.g.*, 73 PA. CONS. STAT. § 2303 (2016) ("An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and un-redacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person."). Along with businesses, "entity" includes "a political subdivision of the Commonwealth."
8. This is the case in Connecticut, New Jersey, Pennsylvania, and Puerto Rico.
9. Only one state, Connecticut, requires by law that a breached entity offer one year of identity theft prevention and mitigation services to its residents. *See* CONN. GEN. STAT. § 36a-701b (2016).
10. Because most fraud losses are refunded by banks and credit card companies, plaintiffs' privacy claims have been limited by holdiing that they lack standing because they have failed to suffer actual injury. *See* Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 365 (M.D. Pa. 2015) ("Allegations of increased risk of identity theft are insufficient to allege a harm."); In re Zappos.com, Inc., 108 F. Supp. 3d 949, 955 (D. Nev. 2015) (collecting cases). Some courts have held, however, that plaintiffs can state a claim arising out of a data breach. *See* In re Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) ("Plaintiffs have alleged ... injuries, including unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees."). These contrasting holdings have created a split of decisions between the federal circuits. The Supreme Court may be asked soon to resolve whether plaintiff's have Article III standing when injury is expressed as an increased risk of future fraudulent charges or other "imminent" harm.
11. Breach notification laws in eight states extend to paper as well as electronic records (Alaska, Hawaii, Indiana, Iowa, Massachusetts, North Carolina, Washington, and Wisconsin).
12. Herbert A. Simon, *Designing Organizations for an Information-Rich World*, COMPUTERS, COMMUNICATION, AND THE PUBLIC INTEREST, 40–41 (Martin Greenberger ed., 1971). ML



A Focus on Recent Qualified Immunity Cases

By Amanda Kellar, IMLA Associate General Counsel and Director of Legal Advocacy

IMLA has recently participated as an amicus in a couple of important Section 1983 / qualified immunity cases that are highlighted below. But before diving into those, in case you missed it, the Supreme Court issued a favorable decision in in *U.S. Army Corp of Engineers v. Hawkes*, concluding that a jurisdictional determination (JD) is a "final agency action" and therefore appealable in federal district court under the Administrative Procedure Act. This was a victory for IMLA, as we joined an amicus brief in the case submitted by the SLLC.

In this case, the Hawkes wanted to mine peat from wetland property in Minnesota. The Army Corp of Engineers issued a JD that the property constitutes "waters of the United States" per the Clean Water Act, meaning the Hawkes would have to obtain a permit to discharge dredged or fill materials into these "navigable waters." Notably, the Corp concluded the property was connected by culverts and unnamed streams to a traditional navigable water way some 120 miles away.

An approved JD – i.e., one finding there are not waters of the United States on the property - is binding on both the Corp and the EPA for five years. Where waters of the United States are found on the property, like in this case, the property owner has the option to apply for a permit. In *Rapanos* (2006) the Court stated that a permit application takes on average 788 days and costs about $275,000. Alternatively, the property owners could choose to forego a permit and commence mining the peat from their property, but in so doing, they could face high civil and criminal penalties under the Clean Water Act.

The Hawkes commenced an action in district court challenging the JD. The Army Corp of Engineers argued that the JD was not a "final agency action" and therefore not subject to judicial review under the Administrative Procedure Act. The Eighth Circuit disagreed and ruled that the Hawkes could seek judicial review of the JD.

In a unanimous opinion authored by Chief Justice Roberts, the Court upheld the Eighth Circuit's ruling, concluding that JDs are final agency action appealable under the APA. The Court explained that under *Bennett v. Spear*, in order for agency action to be considered "final" under the APA it must satisfy two conditions: (1) it must "mark the consummation of the agency's decisionmaking process"; and (2) "the action must be one by which rights or obligations have been determined, or from which legal consequences will flow."

Here, the Corp argued that the second prong was not met, however, the Court disagreed. On this point, the Court reasoned that legal consequences flow from a JD indicating that the property does not contain waters of the United States as it would bind the Corp and the EPA for five years, thus preventing them from bringing any litigation against the property owner during that time and thereby limiting any penalties / damages the property owner would face in that time period. Conversely, a JD, like the one at issue here, that finds that waters of the United States do exist on the property, creates legal consequences as well – the property owner no longer has that five-year safe harbor from liability and instead they risk significant criminal and civil penalties if they decide to discharge onto their property without obtaining a permit.

The Corp also argued that the APA should not apply because the property owners had alternatives to review in court – they could discharge and fill without a permit or they could apply for a permit. The Court rejected this argument as well, indicating that the risk of serious criminal and civil penalties – up to $37,500 per day, is not an adequate remedy nor is it adequate to apply for a permit that the Corp itself told the respondents would be long, arduous and expensive.

Turning to IMLA's recent Section 1983 cases, IMLA will be filing an amicus brief in *District of Columbia v. Wesby*, a certiorari stage Supreme Court case involving the question of whether a police officer assessing probable cause is entitled to credit one set of conflicting statements over another and if the officer cannot, whether the law was clearly established on this point for the purposes of qualified immunity.

In this case, the District of Columbia Metropolitan Police Department received a late night complaint about a loud party and possible illegal activities inside a house that reportedly had been vacant for several months. Officers soon arrived at the home and heard music coming from inside. When the officers knocked and entered, the people inside scattered into different rooms and hid. Police found 21 people throughout the house. The officers observed activity like that "conducted in strip clubs for profit." Consistent with being a vacant property, the house was in "disarray" and essentially unfurnished.

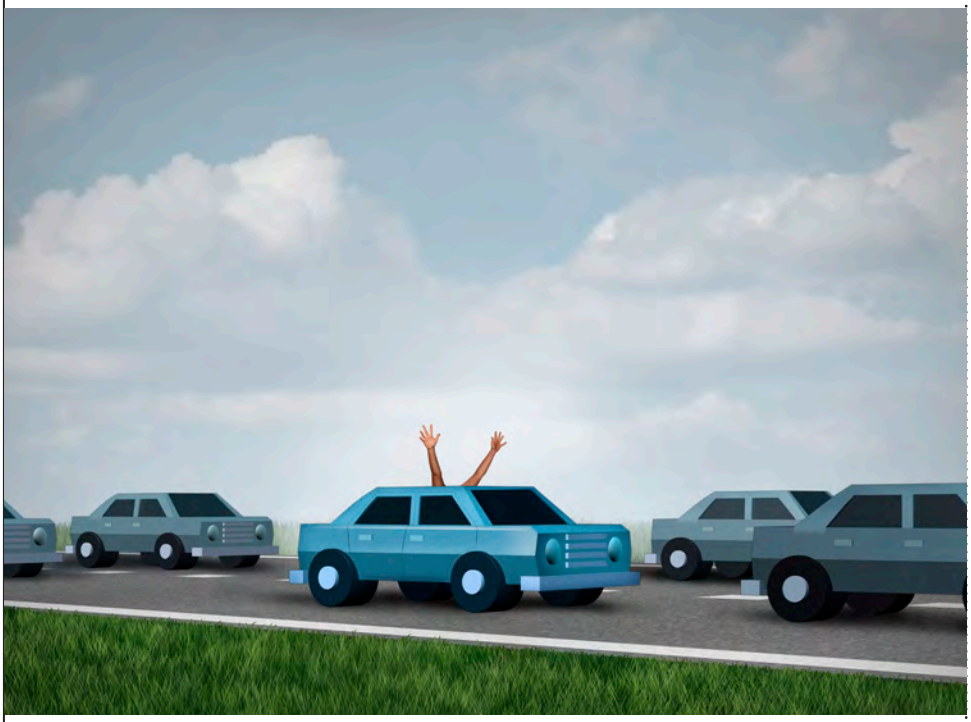
Police gathered information and interviewed all persons present. No one present owned the house, or even knew who the owner was. Some told police that they were there for a birthday party, while others claimed it was a bachelor party. No one could identify the guest of honor. Several said that they had been invited by other people, and some said that a woman known as "Peaches" had given them permission to be in the home. "Peaches," though, was not present.

Officers called "Peaches" on the phone several times but she was evasive and repeatedly hung up. When an officer asked her to come to the home, she refused, explaining that she would be arrested if she did so. "Peaches" informed the police that she had told the partiers that they could use the home. She also initially claimed to police that the owner had given her permission to use the home and that she was

Continued on page 29

The Good, (Potentially) Bad, and (Avoiding) the Ugly: The Benefits, Challenges, and Opportunities Driverless Vehicles Offer to Municipalities

By Gregory Rodriguez, Best Best & Krieger, Washington DC



New innovative and transformative technologies are being incorporated into our transportation networks at a fast pace. No longer are we just talking about laying more concrete for roads as we discuss the future of transportation. Instead, we are talking about incorporating transformative technologies, like driverless cars, into our transportation network. While there are still a lot of unknowns concerning the roll-out of autonomous vehicles — including what safety regulations will look like, their potential societal benefits and economic opportunities — their cutting-edge nature have generated a significant and well deserved amount of "buzz" over a short period of time. However, since such technology does not fit neatly into any existing regulatory framework,[1] we are seeing a traffic jam at the intersection of technology and the law.

Despite the regulatory hurdles, the potential benefits from the smart adoption and rollout of driverless technologies appear to be worth the investment of significant time, money and other resources necessary to bring driverless cars onto the market sooner rather than later. Companies like Google, Lyft, Uber, GM, Toyota, Tesla, Apple and others are racing (and investing significant monetary resources) to position themselves as leaders in the development and testing of this technology. Also, Europe, including the United Kingdom and Germany, China and Australia are also looking to be seen as leaders in the advancement of driverless vehicles.

With the development of driverless vehicles appearing to be well past "first gear," the relevant questions seem to be when, where and how to make sure this technology exists in harmony with our existing transportation network. The correct answers to such questions are critical to preventing a driverless nightmare filled with congestion and counteracting the significant investments and improvements to public transportation made in recent years.

Lay of the Land

Unfortunately, the law often does not move as quickly as technology. Added to that challenge is that governments normally require significant lead time to modify rules, regulations or policies. Throw in human nature's reluctance and suspicion toward adopting significant change and it is easy to discount the predictions that driverless vehicles will be operating on our roads and in our cities within the next 3 to 5 years.

Such skepticism is challenged by the federal lobbying efforts being put forward by companies like Google, Lyft, Ford, Uber and Volvo, which recently announced the formation of the "Self-Driving Coalition for Safer Streets." The purpose of such a coalition is to not only educate lawmakers and regulators about the safety benefits of driverless vehicles, but to also encourage the Department of Transportation and Congress to preempt any state and local efforts to regulate driverless vehicles. The coalition seeks to prevent a "patchwork" of different laws across the country that would hinder the development and roll-out of autonomous vehicles technology.[2] The companies rightly tout the potential safety benefits of truly autonomous vehicles (i.e. no human driver necessary), which include decreased driving accidents from issues like driver fatigue, inattention or drunk driving, and increased mobility for seniors and the disabled. Obviously, such benefits attract the attention of elected officials. (Just watch the Google video and it is hard to be opposed to this technology).[3] However, what is missing from the discussion so far is how any necessary infrastructure to support autonomous vehicles will be paid for, and how to guarantee lower income citizens get to enjoy the benefits this revolutionary technology offers.

Earlier this year, the National Highway Traffic Safety Administration held two public hearings (one at DOT and another in Stanford, Calif.) concerning its development of guidelines for the safe deployment and operation of automated vehicle safety technologies. In a policy statement, DOT and NHTSA stated that the agencies seek "to facilitate and encourage wherever possible the development and deployment of technologies to save lives."[4] In monitoring the recent NHTSA hearings, one sees the challenges that federal and state regulators are facing – autonomous vehicles are more

than licenses, seatbelts and anti-locking breaks. Instead, this technology also crosses into the world of privacy, cybersecurity and moral ethics (i.e. who has the right to program a vehicle to choose between hitting a child who runs into the street and saving the four passengers in a driverless car). Such issues cannot be tied up neatly in a bow in a regulatory scheme and any adopted regulations will need time to adapt as this technology evolves with increased testing and use.

While the federal government is addressing complicated regulatory issues like whether human drivers will be necessary or not in driverless vehicles to be able to "take back" control of a vehicle, many states are positioning themselves to encourage the testing and development of autonomous vehicle technology in their jurisdictions.[5] Cities, including Beverly Hills, Calif., are also taking note of the potential social and economic benefits that autonomous vehicles may provide and seeking the development of municipal-owned autonomous fleets.[6] Such fleets can have various uses, including overcoming the "first and last mile" for getting passengers to public transit stations rather than building costly new transportation infrastructure.

As federal laws and regulations are put forward and enacted, preemption issues are inevitable. The question is how far will the federal government reach in its regulations. Obvious areas of appropriate regulation involve vehicle safety, roadway design and markings to ensure continuity across state lines, and privacy and cyber-security regulations. However, what about issues associated with land use planning, insurance and traffic circulation that are typically under state or local control? As the technology is tested and improved, regulations will need to be flexible enough to evolve while still providing certainty and safety – not an easy endeavor that is being grappled with at the federal level by DOT and NHTSA. Additionally, with the expected large amount of (and potentially expedited) rulemakings at the federal level, it is important for states and local governments to closely monitor and be prepared to participate in the rulemaking process. Local governments should be proactive in protecting state and local interests, since states, counties and cities are the ones that will need to ultimately live with this technology operating on their roads. Smart planning through collaboration now will help ensure the effective roll-out of this exciting technology and help foster the full realization of its potential benefits.

Overcoming Potential Hurdles Through Smart Planning

While it is easy to get lured into inaction thinking driverless vehicles are just a pipe-dream, there are things local governments can start planning for and discussing today to prepare for a driverless vehicle reality. At the very least, all signs point to there being more driverless vehicles on our roads in the near future through the increased testing of autonomous vehicles. By thinking about how the issues below fit into the long-range plans of a public agency, public agencies may be able to save time and resources and ensure the roll-out of autonomous vehicles is smooth.

Land Use Planning: Driverless vehicles have the ability to continue the ongoing transformation of our cities that comes with increased urbanization and centralized living. Increased population in cities has also brought with it increased congestion. Driverless vehicles provide a viable solution to helping address the congestion issue, but only if incorporated into our transportation network in a way that promotes decreased vehicle miles traveled.

When thinking about driverless cars, the idea of no one owning cars arguably promotes the most efficient use of autonomous vehicles. There will no longer be as much need for parking; however, drop off and pick up zones will need to be incorporated into city planning. Unneeded street parking can be used for more bike lanes, and parking structures can be turned into new development, including more affordable housing. The timing of the growth in popularity of ridesharing plays well into a world of no-car ownership.

One potential legal issue that arises in this scenario is how to mandate that no one is able to own cars, especially since Americans do not like freedoms taken away — despite most cars sitting dormant more than 90 percent of the time, according to some estimates.[7] Many are confident that the reduced congestion and more efficient movement in a world of driverless cars will convert any naysayers over time. As testing of autonomous vehicles through pilot projects supported with federal funding[8] grows, do not be surprised to see cities adopt "autonomous only" zones. Such zones make sense in some areas, for instance near stadiums or arenas, to maximize the efficient movement of many people in one place. Such autonomous zones also promote the creation of "Innovation Areas," which can be prime economic opportunities for revitalizing former industrial areas.

Of course, while progressive ideas like less parking structures and more affordable housing sounds wonderful, there is little discussion of how local governments will have the legal means and resources to purchase parking lots and structures through eminent domain. Taking property is not a cheap endeavor given the low overhead and high profitability of parking lots and structures. Moreover, one can feel the rumblings of *Kelo*[9] and the suspicion of some property owners as to whether such use of eminent domain would indeed be for a "public purpose."

The myriad land use issues demonstrate the need for cities and counties to work with municipal planning organizations to update long-range and general plans to include discussions on land use considerations that come with driverless cars. These include those briefly touched on above, as well as the potential elimination of traffic signals, the need for more sensors in roads and promotion of increased density without parking requirements.

Economic Impacts: As noted above, one of the most important details left out of the ongoing driverless vehicle conversation is who is going to pay for any necessary infrastructure to support the safe operation of autonomous vehicles. Such a discussion becomes even more essential when you consider that autonomous vehicles will likely

Continued on page 20



Gregory Rodriguez is of counsel in Best Best & Krieger LLP's Municipal Law practice group and strongly believes that public transportation helps communities become more efficient, increases overall happiness, and promotes connections.

Working out of the firm's Washington, D.C. office, Greg provides guidance concerning federal grant and contracting requirements, and counsels clients on the latest legislation and funding opportunities related to transportation infrastructure.

The Good, The Bad, The Ugly, Cont'd from page 19

decrease local revenues with the elimination of parking fees, in addition to fewer traffic violations since driverless cars will be programmed to follow all traffic laws. Any decreased revenues at a time when there is no long-term funding strategy for transportation infrastructure needs beyond 2021 makes the infrastructure funding question even more pressing.

One potential solution to the forthcoming infrastructure funding dilemma is more "consumption" based taxes, such as the user tax based on miles traveled proposed in the recently enacted Tennessee autonomous vehicle law.[10] Another option is smart tolling for the use of managed lanes dedicated for use by driverless cars. One can also see a type of "franchise fee" system where autonomous vehicle manufacturers/operators pay for the "build-out" of any necessary infrastructure in exchange for a local government allowing driverless cars to be operated within the jurisdiction of a municipality. No matter what the agreed upon solution, it is an issue that cannot be ignored by local governments and an issue that local governments need to be raising right now with federal lawmakers and regulators.

An often difficult consequence of innovation and automation is job losses. The discontent that comes from such job losses is real and can be seen in the ongoing presidential election. Accordingly, another potential economic impact is the numerous job losses of cab drivers and in the ridesharing and long-haul trucking industries, in addition to public transportation operators. While it is easy to discount such unemployment realities by saying new technologies and innovation create new jobs, the people who will lose jobs will be left behind without job retraining programs that ensure they have the skills to succeed in a more technology focused world. Again, it is local governments that will have to accommodate such potential unemployment issues, thus making planning and coordination now with federal lawmakers and regulators necessary and appropriate.

Privacy and Operational Concerns: With technology comes large amounts of data collection. Data collection by local governments can lead to mistrust and scrutiny if clear privacy policies are not enacted and kept up to date. Such policies should make it clear what data is being collected, how it is being used to improve lives and city operations, and how it is being stored and purged.

Driverless cars present both privacy and cybersecurity concerns, especially if increased testing demonstrates that having vehicles connect to a central network improves their safe and efficient operation. However, having cars connect to a system maintained by a local entity creates a significant liability issue, especially from the cyber-security perspective. While this issue is still playing out, the issues of privacy and cybersecurity will be a major part of any discussion at the federal level. In fact, Sen. Ed Markey (D-MA) and Sen. Richard Blumenthal (D-CT) introduced the "SPY Car Act of 2015"[11] that requires compliance with mandated cybersecurity standards seeking to protect all driving data collected by cars and to prevent the hacking of vehicles. Additionally, calming any consumer concerns associated with privacy and cybersecurity will also be tantamount to obtaining and maintaining consumer confidence in driverless cars.

Moreover, we are now seeing an important debate between the automotive and broadband world over spectrum. The broadband that may be needed to support vehicle-to-vehicle and vehicle-to-infrastructure communications to ensure safety must reconcile the wireless industry's desire to continue to meet the needs and expectations of consumers for fast and reliable wireless connections.[12] Such a debate becomes even more important as federal, state and local governments rightly seek to increase connectivity to all citizens.

Such complicated and delicate issues will require diligence by local governments in keeping policies updated and may create new cyber liabilities that will require discussions of risk mitigation options. The insurance industry is already evaluating and preparing itself for the potential exposures that will likely come with driverless vehicles hitting our streets.

Review Existing Laws: A leading legal thinker in the world of autonomous vehicles has proposed that governments perform a "legal audit" to identify and analyze every potential existing statute or regulation within a jurisdiction that may apply to driverless cars.[13] While time consuming and a use of resources, such an approach makes sense, especially when considering that driverless cars cross legal borders into areas like safety, licensing, insurance, privacy, commercial uses and land use regulation. Accordingly, such a legal review will likely benefit governments by identifying areas of potential ambiguity and potentially assist in promoting discussions between interested parties about the safe operation of this technology in states, counties and cities. It would not be surprising to see that the most viable and simplest approach would be the adoption of an "Autonomous Vehicles Code," which would of course need to be consistent with any federal regulations that are adopted.

By understanding and working to address any potential inconsistencies now, the necessary public outreach can be completed in an organized and informed manner. This will help elected officials better understand potential concerns and develop solutions that are accepted by the community. In turn, such work now reduces the risk of lawsuits associated with the implementations of new programs, policies or regulations supporting and encouraging the use and development of autonomous vehicles. With the economic opportunities that new technologies bring with them, such as the conversion of closed down military bases into driverless vehicle testing areas, cities will likely want to be prepared to take advantage of opportunities to promote the testing, development and production of driverless cars in their jurisdictions.

There are indeed significant legal, regulatory, social and economic speed bumps toward the widespread adoption of driverless cars. But the potential benefits are too great to not work collaboratively in successfully incorporating this technology into our existing transportation network. It will not be a simple task, but neither was the invention of the airplane, going into space or climbing Mt. Everest. The recent words of Pres. Obama in Hiroshima offer some insightful words toward the adoption of autonomous vehicles into our transportation network, "[t]echnological progress without an equivalent progress in human institutions can doom us."

The autonomous vehicle challenge has been accepted and cities need to start planning and make sure their voices are heard so they are not left in the rear view mirror when it comes to ensuring safety and money for building any necessary in-

frastructure. Only through smart collaboration and planning can we ensure the full benefits of this technology are realized across all citizens and demographics.

Notes

1. Review of Federal Motor Vehicle Safety Standards (FMVSS) for Automated Vehicles; report by U.S. DOT Volpe National Transportation Systems Center, by Anita Kim, David Perlman, Dan Bogard and Ryan Harrington, Technology Innovation and Policy Division; Preliminary Report – March 2016
2. *See* witness testimony from "Hands off: The Future of Self-Driving Cars" hearing held by Senate Committee on Commerce, Science, and Transportation; March 15, 2016.
3. Google Self-Driving Car Project; https://www.google.com/selfdrivingcar/
4. DOT/NHTSA Policy Statement Concerning Automated Vehicles" 2016 Update to "Preliminary Statement of Policy Concerning Automated Vehicles."
5. See list of enacted and pending autonomous vehicle legislation by states prepared by National Conference of State Legislators; http://www.ncsl.org/research/transportation/autonomous-vehicles-legislation.aspx
6. Beverly Hills: Driven by Innovation; www.drivenbyinnovation.org.
7. "'Cars are parked 95% of the time'. Let's check!" by Paul Barter, posted on Reinventing Parking, Feb. 22, 2013; http://www.reinventingparking.org/2013/02/cars-are-parked-95-of-time-lets-check.html
8. Pres. Obama proposes $3.9 billion over 10-years to accelerate development and adoption of safe vehicle automation through real-world pilot projects; Jan. 14, 2016 DOT announcement.
9. Kelo v. City of New London, 545 U.S. 469 (2005).
10. Tenn. Senate Bill 1561, enacted 5/2/16 as Pub. Ch. 927.
11. United States Senate Bill S.1806; introduced 7/21/15.
12. FCC Proceeding No. 13-49 re Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure Devices in the 5 GHz Band.
13. "How Governments Can Promote Automated Driving," by Bryant Walker Smith (March 17, 2016). ML

Public Safety Technologies, Cont'd from page 13

65. *See* ACLU, *Biometrics*, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/biometrics (last visited June 9, 2016).
66. Timothy Williams, *Facial Recognition Software Moves From Overseas Wars to Local Police*, N.Y. Times, Aug. 12, 2015, http://www.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local- police.html?_r=0.
67. *See* Phil Ross, *Biometrics: A Developing Regulatory Landscape for a New Era of Technology*, Genomics' L. Rep. (May 21, 2014) http://www.genomicslawreport.com/index.php/2014/05/21/biometrics-a-developing- regulatory-landscape-for-a-new-era-of-technology/.
68. Justin Lee, *States Considering Biometrics Capture Laws May Look to Illinois Privacy Laws*, Biometric Update.com (Aug. 5, 2015) http://www.biometricupdate.com/201508/states-considering-biometrics-capture-laws-may-look-to-illinois- privacy-laws. *See* Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1, et seq. and Tex. Bus. & Com. Code Ann. § 503.001.
69. Justin Jouvenal, *The New Way Police are Surveilling You: Calculating Your Threat 'Score'*, Wash. Post, Jan. 10, 2016, https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you- calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html.
70. Although unstated in the article, nearly every police department would have easy access to this type of information from traditional sources like state and federal criminal history data banks ("rap sheets") and internal intelligence.
71. *See* Matt Cagle, *This Surveillance Software is Probably Spying on #BlackLivesMatter*, ACLU (Dec. 15, 2015), https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter.
72. Sarah Burris, *What's Your Threat Score*, ALERTNET (Jan. 14, 2016), http://www.alternet.org/civil-liberties/whats-your-threat-score; Jay Stanley, *Eight Problems with Police "Threat Scores,"* ACLU (Jan. 13, 2016), https://www.aclu.org/blog/free-future/eight-problems-police-threat-scores.
73. See Williams *supra* note 66.
74. See Stanley *supra* note 72. ML





The FDA's First E-Cigarette Regulation

By Caitlin Cutchin, IMLA Associate Counsel

On May 5, 2016, the FDA announced its issuance of a final rule regarding e-cigarettes, further extending its authority to regulate tobacco products. The rule is set to take effect 90 days after its issuance, but provides additional time for e-cigarette producers to comply with new registration requirements. With broad implications for the tobacco industry and public health, this rule—totaling 499 pages—represents the first time e-cigarette producers have been subjected to federal regulation since their emergence on the market and growth in popularity.[1]

Regulatory History and Legal Authority

The FDA's authority to regulate e-cigarettes originates from the Family Smoking Prevention and Tobacco Control Act of 2009 ("TCA").[2] The TCA enables the FDA to regulate the manufacture, distribution, and marketing of tobacco products,[3] and adds Chapter IX to the Federal Food, Drug, and Cosmetic Act ("FDCA").[4] Chapter IX of the FDCA applies to all cigarettes, cigarette tobacco, roll-your-own tobacco, and smokeless tobacco and to any other tobacco products the Secretary of Health and Human Services, by regulation, deems to be subject to the FDCA.[5] Through the utilization of the Secretary of Health's deeming authority, the FDA's new rule expands the FDCA's definition of "tobacco product" to include e-cigarettes.[6]

Requirements

Under the new rule, e-cigarette producers, like the producers of traditional tobacco products, will not only be required to register with the FDA and provide a detailed account of their ingredients and manufacturing processes, but they will also be required to apply for permission from the FDA to sell their products.[7] This requirement will include local "vape shops" that mix their own e-cigarette liquid, causing some controversy among smaller producers that argue they will not have the same resources as larger tobacco companies to navigate the FDA's two-year compliance period and application process.[8]

Under the new regulations, all producers will also be required to seek FDA approval before marketing their e-cigarette products as "light" or "mild." Further, companies will also be prohibited from handing out free samples. While the published rules do not include a specific ban on flavors in e-cigarettes, health officials have indicated that they are working on new rules to extend the flavor bans for traditional cigarettes to cigars.[9] Antismoking activists have expressed disappointment in the absence of flavor bans within the new regulations.[10] The rule's executive summary indicates the FDA's intent to balance "concerns regarding flavored tobacco products' appeal to youth" with "emerging evidence that some adults may potentially use certain flavored tobacco products to transition away from combusted tobacco use."[11]

In addition to production requirements, the new rules also establish new youth-access restrictions for "covered tobacco products"[12] including: (1) Requirement for minimum age of purchase; (2) Requirement for health warnings for product packages and advertisements; and (3) Prohibition of vending machine sales of such products, unless the vending machine is located in a facility where the retailer ensures that individuals under 18 years of age are prohibited from entering at any time.[13]

Constitutional Issues

During the required notice and comment period, members of the public raised several concerns regarding the constitutionality of the promulgated rule. Stakeholders, largely members of the tobacco industry, criticized the new regulations for infringing upon their commercial speech rights—namely, their ability to give out free samples.[14]

In response, the FDA argues that the distribution of free samples is conduct, not commercial speech. The FDA argues that under *Arcara v. Cloud Books Inc.*,[15] "provisions that regulate conduct without a significant expressive element do not implicate the First Amendment."[16] Further, the FDA also points out that in *Discount Tobacco City & Lottery, Inc. v. United States*, the 6th Circuit upheld a ban on free samples of tobacco products, despite holding that free samples constituted commercial speech, because the government had sufficiently demonstrated that the ban would directly and materially advance the government interest of decreasing use of tobacco products by youth.[17]

Other stakeholders express concern that the new regulations will replace state and local laws already in place to limit tobacco product availability and promote public health. Specifically named in the comments was California's reproductive health warning requirements, as passed by Proposition 65 in 1986.[18]

In response to these comments, the FDA states that under FDCA § 387p(a)(1), states and local governments have broad latitude to regulate tobacco products, allowing federal agencies, states, and Indian tribes the ability to "enact, adopt, promulgate, and enforce any law, rule, regulation, or other measure relating to or prohibiting the sale, distribution, possession, exposure to, access to, advertising and promotion of, or use of tobacco."[19] Federal requirements regarding product standards, pre-market review, adulteration, misbranding, labeling, registration, good manufacturing standards, and modified-risk

Continued on page 32



Suggestions and Forms for Objections to Requests for Production under the Amended Federal Rules

By Pete Haskel, Executive Assistant City Attorney, Dallas, Texas

Here are some suggestions and forms for objections to requests for production ("RFP") under the Federal Rules of Civil Procedure as amended effective December 1, 2015 ("Rules"). IMLA's eDiscovery and Legal Hold Working Group is drafting a more comprehensive set of model preservation and discovery motions, objections, demands, and responses under the amended Rules for prelitigation and pretrial use, but here are my preliminary thoughts respecting RFP objections. There is some repetition here because I intend this to be a quick reference and therefore for the reader's convenience I repeat points where they are relevant:

The Rules treat documents and electronically stored information ("ESI") as two different things – so your objections should observe the distinction, even where RFP definitions or instructions confute or combine the two (*e.g.* a definition stating: "'Documents' includes ... 'electronically stored information'"). This distinction can become significant. For example, there is a specific provision allowing for cost shifting before a party must collect and review ESI that is not readily accessible because of undue burden or cost. Fed. R. Civ. P. 2(b)(2)(B). There is no explicit counterpart for paper documents.[1] Also, a requester must specify the format of ESI production – "If the responding party objects to a requested form—or if no form was specified in the request—the party must state the form or forms it intends to use." Fed. R. Civ. P. 34(b)(2)(D).

Avoid reliance on general objections. The rules require specific objections: Fed. R. Civ. P. 34(b)(2)(B) ("For each item or category, the response must either state that inspection and related activities will be permitted as requested or state *with specificity* the grounds for objecting to the request, including the reasons" (emphasis added)). The courts are starting to treat general objections as waiving objection to specific RFPs, particularly if the general objection is couched in terms of objecting "to the extent that the objection applies."[2]

The easiest way to comply with the specificity requirements for objections is to set out each definition, instruction, and RFP verbatim in the response and objections, with individual objections set out as to each such item. In other words, treat definitions and instructions the same way we treat the actual requests in preparing responses and objections. For example, an objection to a definition would appear immediately after the text of the definition objected-to, and the objection would start with words to the effect, "Defendant objects to the definition immediately above on the grounds that ...." However, each such objection should be restated or incorporated by reference in specific objections to each RFP affected by the defective definition or instruction. So the objections to each defective instruction or definition should restate the objections to the definitions and instructions that apply to that RFP.

For example, here is an objection to a specific definition: "This overly broad definition of "You, Your, and City of XXX" renders each RFP in which the definition is used too vague and ambiguous to permit a response and so overbroad that it exceeds the permissible scope of discovery under Fed. R. Civ. P. 26(b)(2) as demonstrated below as to each such RFP."

Define each objection that you will use again. For example, the first objection to an overly broad definition of "You" Your, or City of XX" could be followed by the parenthetical definition, "(the 'Overbroad City Definition' or 'OCD')."

Thereafter, restate the objection after each associated RFP (either by pasting the objection and adapting it to the RFP or, preferably, by incorporating by reference using the definition for the objection), the specific objections that apply to each RFP. For example, a term that is rendered overbroad by an overbroad definition would include sentence, "Defendant further objects to this RFP on the grounds of the OCD Objection."

To the extent that your incorporated or restated objection attacks proportionality, undue burden, or other fact-specific defect, we must in addition to stating the specific objection provide objective factual bases for the objection. Usually we need affidavits from records custodians and IT personnel to estimate how much time and expense the objectionable search would require.

Even when an objection does not stem from a general objection to instructions or definitions, carefully tailor objections to facts of the case–do not use cookie-cutter objections–and demonstrate how each objection relates specifically to each RFP for which the objection is asserted.

Always attach affidavits or other evidence that establish the facts to support your objections – courts are rejecting conclusory objections.

Do not state that your client will produce documents or ESI "subject to" objections. Recent rulings and the recent Rules amendments demand that the objector make clear whether documents or ESI are actually being withheld. *See* Fed. R. Civ. P. 34(b)(2)(B) (objecting party must state if documents or ESI will be produced or made available for inspection for each category). Courts

Continued on page 32



Cases of Interest

By Monica Ciriello, Ontario 2015

Municipal Tax Reduction Granted Due to Sickness

A.P. v. Toronto (City), 2016 CanLII 28435 (ON ARB) http://canlii.ca/t/grqfm

The Applicant appeared before the Assessment Review Board ("Board") relying on s. 323 (1)(e) of the *City of Toronto Act, 2006* ("*Act*") requesting that his property taxes be cancelled during the 2014 taxation year due to sickness or extreme poverty. The City of Toronto opposed the application.

HELD: The Applicant qualified for a tax reduction due to sickness.

DISCUSSION: In this case, the Board applied the two-part test found in section 323(1)(e) of the *Act*. The Board first examined the evidence presented by the Applicant to determine whether or not sickness or extreme poverty existed. The Board relied on a note presented by the Applicant in which a doctor stated that the Applicant had been unemployable since 2005 due to hepatitis and cirrhosis of the liver, and was satisfied that the element for sickness was proven. The Board next considered if it was the Applicant's sickness during the 2014 taxation year that prevented him from paying the property taxes. With respect to this second part of the test, the Board wrote that,

> The *Act* envisions that an individual seeking relief on application under s. 323 of the *Act* should clearly demonstrate that for the year under appeal, the Applicant, after scrupulously managing his/her resources and expenditures, was left with no resources available to meet some or all of his/her property taxes.

The Applicant presented evidence that his sole income was from Ontario Works and the Ontario Disability Support Program in the amount of roughly $1,300 per month, and he also received a 'low income rebate' on his hydro bill. His monthly expenses exceeded $1,900 per month. He was unable to generate any other income due to his health. He owed his son more than $135,000 which was secured by a mortgage against his home, valued at approximately $507,000. The son was the only mortgagee on the home and was the sole beneficiary under the Applicant's will—and was not pressing for foreclosure despite Applicant's being in arrears. After reviewing the Applicant's financial data, including the fact that Applicant had equity in his home, the Board concluded that the Applicant's sickness did not completely prevent his paying any property taxes for the 2014 taxation year. However the Board did permit a reduction of $329.10 as relief under the *Act*.

New Trial for City Found Guilty Under the Occupational Health and Safety Act; Separate Actus Reus Must Be Proven for Each Offence

R. v. St. John's (City), 2016 CanLII 28455 (NL SCTD) http://canlii.ca/t/grqhn

In 2011, two employees from the City of St. John's ("City") were inspecting asphalt along the Trans-Canada Highway with employees from Irving Oil and the provincial government. While inspecting the asphalt, two employees – one from Irving Oil and one from the City- were injured after being hit by an oncoming vehicle. Another employee from the provincial government was killed. The City and the Department of Transportation and Works ("DTW") were charged under the *Occupational Health and Safety Act*, R.S.N.L. 1990, c O-3 ("*Act*") for numerous violations, including the failure to use appropriate safety procedures, failure to provide effective traffic control, failure to provide adequately visible workplace clothing and so on.

At trial the City argued that a careless driver caused the injury to its employee. They claimed that the accident could not have been prevented regardless of any protection or training requirements under the *Act*. Therefore, the City could not have breached the *Act*. The Provincial Court found the City and the DTW guilty of all seven charges under the *Act*, holding that "the fact of a workplace accident which takes place while an employee is engaged in the work of the employer and which accident is related to the performance of the work of the employer is sufficient to provide proof of the *actus reus* of the offence in question." The City appealed; the DTW did not.

HELD: The appeal was allowed and a new trial ordered.

DISCUSSION: The City's trial argument was echoed on appeal, asserting that the trial judge committed various legal errors. While recognizing that the *Act* was to be liberally construed so as to promote safety, the Justice was not willing to overlook basic procedural legal standards. He agreed with the City that it was an error on behalf of the trial judge to conclude that the employees being hit by an oncoming vehicle established *prima facie* proof that rose to the level of requiring the City to prove due diligence. The Justice also found that the trial judge erred by applying the same *actus reus* from the first charge to all seven charges and failed to examine the factual elements for each of the different charges. The Justice stated that, "for each offence, the *actus reus* must be proven before any issue of the employer's due diligence becomes relevant" and because the trial judge failed to require each count to be proven, the appeal was allowed:

> Since this approach, with its emphasis on the consequences of any breach rather than on the identification and proof of the actual elements of each breach, permeated the whole conduct of the trial and the adjudication itself, the convictions cannot stand. Proof of the *actus reus* of each offence was found based on a faulty legal premise and without differentiation between the counts. In the circumstances it is not appropriate to enter an acquittal and a new trial should be ordered.

Unjustified Invasion of Personal Privacy: The Application of the Municipal Freedom of Information and Protection of Privacy Act.

Mississauga (City) (Re), 2016 CanLII 24077 (ON IPC) http://canlii.ca/t/gr4zb

The City of Mississauga ("City") received a request under the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O 1990, c F.31 ("*Act*") from the Appellants pertaining to complaints and opinions filed with the City about hedges, standing water and other elements of Appellants' property. The City provided the Appellants with partial access to the records as permitted under the *Act*. The Appellants appealed.

HELD: The appeal was dismissed.

DISCUSSION: The adjudicator began by examining section 2(1) of the *Act*, to determine whether the records contained personal information about the complainants. Relying on *Ontario (Attorney General) v. Pascoe*, 2002 CanLII 30891 (ON CA) which found that,

To qualify as personal information, it must be reasonable to expect that an individual may be identified if the information is disclosed.

The adjudicator concluded that personal information of both the Appellants and the complainants were in the records. Next, section 38(b) of the *Act* was dissected to determine whether the personal information in the records "would constitute an unjustified invasion of personal privacy of the complainants" even if it contained personal information of the Appellants. And therefore, this was used to justify the City's refusal to disclose the records. The adjudicator relied on section 14(2) and (3) of the *Act* to determine if disclosing the records to the Appellants would rise to the level of unjustified invasion of privacy. Under section 14(2) the Appellants must establish all elements of a four-part test in order to justify obtaining access to personal information in support of an asserted right: (1) the right in question is a legal right which is drawn from the concepts of common law or statute law, as opposed to a non-legal right based solely on moral or ethical grounds; and (2) the right is related to a proceeding which is either existing or contemplated, not one which has already been completed; and (3) the personal information which the appellant is seeking access to has some bearing on or is significant to the determination of the right in question; and (4) the personal information is required in order to prepare for the proceeding or to ensure an impartial hearing.

The adjudicator found that the Appellants did not satisfy elements three and four, because their case—contesting the validity of allegations about their property—did not hinge upon the identities of the complainants.

Additionally, section 14(3)(b) states,

A disclosure of personal information is presumed to constitute an unjustified invasion of personal privacy if the personal information,was compiled and is identifiable as part of an investigation into a possible violation of law, except to the extent that disclosure is necessary to prosecute the violation or to continue the investigation.

The Appellants did not provide an argument to rebut section 14 (3)(b). The adjudicator concluded that the personal information presumption applied. Applying section 14, the adjudicator concluded that releasing the personal information requested by the Appellants would result in an unjustified invasion of personal privacy under section 38 of the *Act*.

Court of Appeal Lacks Jurisdiction to Review Superior Court Judge Grant of Leave to Appeal Arbitration Decision

Ottawa (City) v. Coliseum Inc., 2016 ONCA 363 (CanLII) http://canlii.ca/t/grnf7

In 2004, the City of Ottawa ("City") and Coliseum, Inc. ("Coliseum") entered into Minutes of Settlement ("Settlement") to resolve a dispute concerning a long-term lease agreement. The Settlement called for arbitration of disputes but did not expressly specify that matters of law would be subject to arbitration. Under the Settlement, the City could terminate the lease if it had *bona fide* plans to redevelop the stadium, in which case the Coliseum would be given an option to lease an alternate City-owned property.

In 2010, the City announced plans to redevelop the stadium, sent Coliseum a Notice to Terminate the lease agreement, and provided an option to lease alternate property. Coliseum ultimately rejected the City's offer and invoked the Settlement's arbitration clause.

The arbitrator granted Coliseum $2,240,000 in damages, finding that the City had failed to offer alternate property which was appropriate to Coliseum's use, as required by the terms of the Settlement.

The City appealed, citing s. 45(1) of the *Arbitration Act*, 1991, S.O. 1991, c. 17, which allows a party to appeal an arbitral decision based on a question of law, provided the arbitration agreement is silent on the issue. The application judge granted leave to appeal and reversed the arbitrator's award, reducing it by 40% and applying the Supreme Court of Canada decision, *Sattva Capital Corp. v. Creston Moly Corp.*, 2014 SCC 53 (CanLII). The application judge found that the arbitrator erred in his interpretation of the Settlement and did not correctly apply the "reasonableness" standard in determining the arbitral award, requiring a reduction of the award by 40%.

Coliseum appealed the application judge's decision to the Court of Appeals (1) arguing that the City should not have been allowed to appeal the arbitration and (2) challenging the reduction of the arbitrator's award.

HELD: The application judge's allowance of the appeal from the arbitrator's decision may not be appealed by Coliseum; however, the application judge's modification of the arbitrator's award may be reviewed for reasonableness and the award reinstated.

DISCUSSION: The first question was whether the Court of Appeal had the jurisdiction to review the application judge's decision granting leave to appeal the arbitral award. The Court relied on the findings in *Hillmond Investments Ltd. v. Canadian Imperial Bank of Commerce*, 1996 CanLII 413 (ON CA) and *Denison Mines Ltd. v. Ontario Hydro*, 2001 CanLII 5681 (ON CA), both of which significantly circumscribe the instances where an appellate court can review a lower court's decision to allow an appeal from an arbitration. The Court of Appeals concluded that it lacked jurisdiction to hear a challenge to the lower court's allowing an appeal of the arbitration. However, the Court of Appeals was not foreclosed from examining the outcome of that appeal—the application judge's reduction of the arbitral award. The Court reversed the application judge's findings that the arbitrator's reasoning was unreasonable, finding that the application judge erred by replacing his interpretation of the Settlement with that of the arbitrator. The Court found that the arbitrator's

Continued on page 32

2016 NOMINATING COMMITTEE



Pursuant to its By-Laws, IMLA announces its 2016 Nominating Committee ("Committee"). The Committee encourages members interested in being nominated for vacant positions on the IMLA Board of Directors ("Board") and for IMLA Regional Vice Presidents to make their interest known to the Committee. In addition to filling vacancies, the Committee is charged with nominating IMLA's officers including Treasurer and President-elect. Some members of the Board are term limited and cannot seek reelection; as a result there will be several vacancies open. It is IMLA's goal that the Board represent IMLA's diversity of region, gender, race, age and ethnicity and welcomes all who wish to serve. Unlike many non-profits, IMLA does not require Board members to contribute financially to the organization, but does seek persons who are interested in advancing IMLA's mission, increasing its membership and attendance at its programs.

The Committee is as follows and will be meeting during the San Diego Annual Conference at the Hilton Bayfront Hotel at a date and time to be announced. Please Contact The Committee In Advance And Plan To Attend The Meeting If You Are Interested In Submitting Your Name Or The Name Of Another Member For Nomination:

Robert S. Croom
Deputy General Counsel
South Carolina Association of Counties
PO Box 8207
Columbia, SC 29202-8207
rcroom@scac.sc

Anthony Fox
Town Attorney
Weddington, North Carolina
Three Wachovia Center
401 S. Tryon Street, Ste. 3000
Charlotte, NC 28202
anthonyfox@parkerpoe.com

Randall Van Vleck
General Counsel
New Mexico Municipal League
PO Box 846
Santa Fe, NM
rvanvleck@nmml.org

JoAngela Woods
General Counsel
Indiana Association of Cities & Towns
Station Place
200 S. Meridian St. Ste. 340
Indianapolis, IN 46225
jwoods@citiesandtowns.org

Byron Werry
City Solicitor
Regina, Saskatchewan
City Hall
P.O. Box 1790
Regina, SK S4P 3C8 Canada
bwerry@regina.ca



The Committee is charged with identifying candidates who will work to increase the value of IMLA to its members, strengthen the organization and ensure the diversity of the Board. IMLA Regional Vice Presidents are also selected by the Committee and it has been IMLA's past practice to nominate the current Regional Vice Presidents unless there is a vacancy. A current copy of IMLA's By-Laws can be found on IMLA's website at www.imla.org. The By-Laws describe the qualifications for service on the Board or other IMLA office. The Board of Directors hopes that all interested members will apply.

IMLA'S BOARD OF DIRECTORS 2015 – 2016: OFFICERS

PRESIDENT

Herbert W.A. Thiele
County Attorney
Leon County, Florida Room 202
301 South Monroe Street
Tallahassee, FL 32301
ThieleH@leoncountyfl.gov

PRESIDENT-ELECT

Mary Ellen Bench
City Solicitor
Mississauga, Ontario 3rd Floor
300 City Centre Drive Mississauga,
ON L5B 3C1 Canada
maryellen.bench@mississauga.ca

IMMEDIATE PAST PRESIDENT

G. Foster Mills
Managing Attorney
New York City, New York (retired)
gfmills53@gmail.com

TREASURER

Andrew J. Whalen, III
City Attorney
Griffin, Georgia - Whalen & Westbury
P.O. Box 133
Griffin, GA 30224
ajwhalen3@whalenlaw.net

GENERAL COUNSEL AND EXECUTIVE DIRECTOR

Charles W. Thompson, Jr.
IMLA
7910 Woodmont Avenue,
Suite 1440
Bethesda, MD 20814
cthompson@imla.org

BOARD OF DIRECTORS

Barbara A. Adams
Village Attorney
Kenilworth, IL
Holland & Knight LLP
131 South Dearborn St. 30th Floor
Chicago, IL 60603
barbara.adams@hklaw.com
Term expires 2016 (Not eligible for reelection due to term limits)

Patrick Baker
City Attorney
Durham, NC
101 City HallDurham, NC 27701
patrick.baker@durhamnc.gov
Term expires 2016

Marianne Landers Banks
Interim City Attorney
Springfield, Missouri
840 Boonville Avenue
Springfield, MO 65802
mbanks@springfieldmo.gov
Term expires 2016 (Not eligible for reelection due to term limits)

A. Rene' Broker
Borough Attorney
Fairbanks North Star Borough
809 Pioneer Road
Fairbanks, AK 99701
rbroker@fnsb.us
Term expires 2016 (Retiring)

Continued on next page

2016 NOMINATING COMMITTEE CONT'D FROM PAGE 27

Tyrone E. Cooper
City Attorney
City of Beaumont, Texas
801 Main Street
Beaumont, TX 77701
tcooper@ci.beaumont.tx.us
Term expires 2016

Robert S. Croom
Deputy General Counsel
South Carolina Association of Counties
PO Box 8207
Columbia, SC 29202-8207
rcroom@scac.sc

Gary Ebert
Director of Law
Bay Village, Ohio
350 Dover Center Road
Bay Village, OH 44140
gebert@cityofbayvillage.com
Term expires 2017

Wayne Esannason
Village Attorney
Scarsdale, New York
Scarsdale Village Hall
1001 Post Road
Scarsdale, NY 10583
wesannason@scarsdale.com
Term expires 2017

Cathy Hampton
City Attorney
Atlanta, Georgia
55 Trinity Ave, Suite 5000
Atlanta, Georgia 30303
cathyhampton@atlantaga.gov
Term expires 2018

Douglas C. Haney
Corporation Counsel
Carmel, Indiana
One Civic Square
Carmel, IN 46032
dhaney@carmel.in.gov
Term expires 2016
(Not eligible for reelection
due to term limits)

Roger Horner
City Attorney
Brentwood, Tennessee
P.O. Box 788
5211 Maryland Way
Brentwood, TN 37024-0788
hornerr@brentwood-tn.org
Term expires 2018

Rose Humway-Warmuth
City Solicitor
Wheeling, West Virginia
1500 Chapline Street
Wheeling, WV 26003
rhwarmuth@wheelingwv.gov
Term expires 2018

Monica Joiner
City Attorney
Jackson, Mississippi
P.O. Box 2779
455 East Capitol Street
Jackson, MS 39207-2779
mjoiner@city.jackson.ms.us

Stephen Kemp
Former City Attorney
Peoria, Arizona
Office of the City Attorney
8401 West Monroe, Room 340
Peoria, AZ 85345
steve.kemp@peoriaaz.gov

Art Pertile
City Attorney
Stafford, Texas - Olson & Olson, LLP
Wortham Tower
2727 Allen Parkway, Ste 600
Houston, Texas 77019
apertile@olsonolson.com
Term expires 2017

Susan L. Segal
City Attorney
Minneapolis, Minnesota
350 South 5th Street, Rm. 210
Minneapolis, MN 55415
susan.segal@ci.minneapolis.mn.us
Term expires 2016 (Not eligible for reelection
due to term limits)

Amicus Cont'd from page 17

"possibly renting" it from him. Soon, though, "Peaches" admitted to the police that, contrary to her initial claim, she lacked the owner's permission to use the home. Police then spoke with the homeowner, who confirmed that the house was vacant and that no one, including "Peaches," had permission to be there.

Police arrested all of the partygoers for criminal trespass (and disorderly conduct – though the petition will focus on criminal trespass), although prosecutors ultimately did not pursue charges.

The partiers brought a Section 1983 claim, claiming the officers lacked probable cause to arrest them for criminal trespass. The district court granted the partiers' motion for summary judgment, finding that their arrests were without probable cause and that the two defendant officers were not entitled to qualified immunity. After a damages-only trial, the district court entered a judgment against the officers (and jointly against the District of Columbia) totaling nearly $1 million.

The District of Columbia Circuit affirmed in a 2-1 decision. It reasoned that the officers did not have "conflicting information" that would overcome the partiers' claim that they had been invited to the house by "Peaches" and therefore no reasonable officer could have believed that the partiers knew or should have known that their entry was unauthorized. (The DC statute for trespass required a culpable mens rea on the part of the trespassers). Thus, according to the Circuit Court, a reasonable officer could not have believed that there was probable cause to arrest the plaintiffs.

The DC Circuit next concluded that the law was clearly established, for qualified immunity purposes, because the legal elements of criminal trespass were clearly established, even though no case had invalidated an arrest for trespassing under similar circumstances. The full panel later denied rehearing en banc, over the written dissent of four judges.

This case presents an important question affecting law enforcement, by imposing a heightened probable cause standard under which officers must credit a suspect's claim of an innocent state of mind for conduct that otherwise appears criminal, even when officers have reasonable grounds to doubt the suspect's credibility. This heightened probable cause standard would make it difficult for police officers to enforce not only trespassing laws, but also any criminal law requiring a culpable mental state. Arresting officers often lack direct proof of a suspect's mental state, while suspects often assert a variety of mens rea-related excuses for apparent criminal behavior. The District of Columbia Circuit's decision would make it difficult to establish probable cause in these circumstances. As Judge Kavanaugh notes in his dissent from the denial for rehearing on this point:

The panel opinion's approach is not and has never been the law. When police officers confront a situation in which people appear to be engaged in unlawful activity, the officers often hear a variety of mens rea-related excuses. "The drugs in my locker aren't mine." "I don't know how the loaded gun got under my seat." "I didn't realize the under-aged high school kids in my basement had a keg." "I wasn't looking at child pornography on my computer, I was hacked." "I don't know how the stolen money got in my trunk." "I didn't see the red light." "I punched my girlfriend in self-defense."

But in the heat of the moment, police officers are entitled to make reasonable credibility judgments and to disbelieve protests of innocence from, for example, those holding a smoking gun, or driving a car with a stash of drugs under the seat, or partying late at night with strippers and drugs in a vacant house without the owner or renter present.

Again, as the dissent points out, this case also runs counter to several recent Supreme Court decisions that have reversed courts of appeals in qualified immunity cases. Contravening Supreme Court precedent, the District of Columbia Circuit defined clearly established law at a high level of generality. Simply because the legal elements of an offense might be clearly established does not mean that police officers are on fair notice whether they have probable cause to arrest for that offense in the particular situation they confront. The Circuit's erosion of the qualified immunity defense will have a chilling effect on law enforcement and make it difficult for them to arrest trespassers and other suspects engaged in crimes where other mens rea type excuses could be made.

The other recent Section 1983 case in which IMLA filed an amicus brief is *Lowry v. San Diego,* a petition for rehearing before the Ninth Circuit. In this case, the appellant, Lowry, went out after work drinking with her friends. After consuming 5 vodka drinks, she decided to go back to her office to sleep on the couch there. At approximately 11 pm, she got up to use the bathroom and unbeknownst to her, triggered the building's burglary alarm. Several San Diego police officers responded within minutes to the alarm, including an officer accompanied by a police service dog.

Upon arriving and inspecting the building, the officers noticed that the door leading to Suite 201 was propped open. There were no signs of forced entry and the suite was dark. Because the officers could not see inside the office suite, they did not know if anyone was inside. Before entering the suite where Lowry was sleeping, the police officers loudly gave the warning: "This is the San Diego Police Department! Come out now or I'm sending in a police dog! You may be bitten!" The officers then waited between 30 and 60 seconds and after receiving no reply, repeated the same warning once or twice more. When there was again no response, the officer let the dog off his leash and entered the suite, following closely behind the service dog.

The officers entered the office where Lowry was sleeping. Once there, one of the officers shone his flashlight against the wall and spotted someone under a blanket on the couch. At that moment, the dog jumped on top of Lowry. The two struggled briefly before the officer called the dog back and the dog responded immediately.

After confirming that Lowry was an employee for the office building, the officers drove her to the hospital where she received medical care. As a result of the dog bite, Lowry had a gash on her lip that required 3 stitches.

Relevant to this incident, the San Diego Police Department trains its police dogs to enter a building, find a person and bite them and hold the bite until the police officer calls the dog off. The dogs are not trained to differentiate between "a young child asleep or ... a burglar standing in a kitchen with a butcher knife." Whether to conduct the search on leash or off leash is generally left to the discretion of the officer, however, the SDPD's manual provides that residential searches (as opposed to commercial ones) should normally be conducted on leash.

Lowry sued the City of San Diego, alleging that the City's policy of training the police dogs to "bite and hold" violated her Fourth Amendment rights. The district court granted the City's motion for summary judgment, finding that the officer did not violate Lowry's constitutional rights under the *Graham* analysis.

The Ninth Circuit reversed, holding that a reasonable jury could find that the force

Continued on page 35



The First Amendment and the Right to Toss Pizzas

By Brad Cunningham, Municipal Attorney, Lexington, South Carolina

Alright, repeat after me... All together now..... In what ways can we regulate signs and / or speech? One... two... three..... "Time, Place and manner of delivery...." This is our mantra..... Right? Well, maybe not so fast.....

One of the more recent "highly discussed" issues on the listserve has been the distribution of flyers, leaflets, handbills, etc... Local Governments continue to be plagued with issues related to and complaints about distributions of these items throughout Town. One such case came to light here in the Town of Lexington when I was first on staff.

A local pizza delivery company had made a practice of throwing a flyer advertising the weekly specials into the yard of virtually every house in Town. The flyers were not enclosed but were "weighted down" by a plastic attachment which actually served no real purpose. The result was debris scattered all over town. In a neighborhood such as mine, with 180 homes, flyers were blowing around in the road, into the pool, into the storm drains and once, even into the grille of a car. Local officials complained of the behavior, and, as expected, the business owner brought up the "freedom of speech" issue. Of course, our local officials responded this was a manner of delivery issue that had nothing to do with the content. The business owner was a small business owner, and claimed this was the only way he could afford to advertise. I advised steering the conversation toward litter and citizen complaints, and away from any discussion of the business. In an effort to please the business owner, a compromise was reached whereby the flyers were to be designed as "placards" and hung on door knobs of residents, instead of being tossed into the yard.

Well, this brought another round of complaints as some homeowners didn't want the representatives coming onto their property and hanging placards on their doors. Also, some of the placards were still being blown off by the wind, and even tossed aside by neighborhood children. So the litter situation was lessened somewhat, but not totally resolved. This went on periodically for months, until later the business finally folded and the owner left town.

My thought still remains this: Why isn't this a relatively easy "manner of delivery" issue regarding regulating the throwing of handbills into the yards of residents? A great number of residents did not want anyone, regardless of the content of the object thrown, to toss unwanted objects into their yards. This is not like a newspaper subscription that a resident might request voluntarily, but in most instances involves unknown persons throwing unwanted objects into residents' yards... It almost appeared that the business was arguing that the First Amendment guaranteed the right to litter.

Is it simply the fact that the object had "words" on it that protected the right to throw it into the yard? Would it have been different if the pizzas themselves were thrown into the yard with no written material on them? Would prohibiting that have been OK since no alleged "speech" was involved? The other issues, littering, etc., would still remain the same. Somehow the throwing of pizzas into the yard appears to be an easier call.... But why? The only real difference is the handbills had words on them. Query: Could the throwing of the pizzas be prohibited by local authorities? Seems plausible, but, again, wait... Not so fast....

We had a number of protesters not long ago who decided their cause was important enough to camp out on the statehouse grounds. Fair enough..... But what was left behind was not fair, and was quite simply a disgusting display of abusing the right to assemble and exercise what was called "free speech." The protesters left behind trash, tents, excrement, you name it, and it was left on the grounds. This same group later planned another demonstration, and when the authorities complained of the behavior from the previous demonstration, out came the "freedom of speech" claims again. Please don't get me wrong, I am no enemy of the First Amendment, by any means. But what I question is the point at which the behavior becomes more than "speech," and becomes actual action. And, in the case of dangerous, unhealthy or disruptive action, it brings many concerns to mind.

"Freedom of Speech" was actually used as a defense to an individual caught using the bathroom on the statehouse grounds... No discussion regarding the content of the speech ever came into play. It just simply was claimed that this was an exercise in free speech. The case actually had some traction at first, but wiser heads prevailed and eventual charges of littering and disorderly conduct were sustained. The penalty was relatively minor.

Once again, I truly and fully support the First Amendment, but I suppose the issue in these cases is deciding at what point an individual exercise of "free speech" becomes more about actions (sometimes harmful) than about words or content. We can stick to the time, place and manner of delivery restrictions, but let's be careful... It doesn't seem to be an easy issue.

A ListServ member recently brought forth another fun question that stirred a lot of interesting conversation. A developer was buying a large parcel to build a neighborhood, and the contract to purchase required the purchaser to preserve certain elements of the property. This contractual obligation to "preserve" bumped heads with city requirements regarding depth of some lots, and with the width of streets. So, the developer sought

a variance, and the question became whether this was a valid reason to grant a variance. The discussion was fun, but most responses leaned toward the idea that a contractual obligation to a third party did not constitute the "hardship" grounds necessary to establish a variance. There was some discussion about the "reason" for the contractual "preservation" of certain elements, but this was largely deemed to be less of an issue than whether the variance request met all that was necessary to comply with state requirements. "It's pretty," or "it's expensive to comply" just don't cut it when requesting a variance. This is especially true when the zoning requirements were in place prior to the signing of the contract. A very good possibility of "side-stepping" the issue was suggested in the form of allowing a Planned Unit Development or "PUD" to be put in place to solve the matter. It appears to have been worth investigating.

But, the overarching concern remains - what happens when a contractual obligation requires an "illegal" act? I certainly don't think such a provision could be applied retroactively-that is, if the contract were in place first and performance had already been achieved. However, in the other scenario, I think folks often run into problems thinking they can "contract" to do almost anything they want. I bring to you another local case in point.

I have served as the Chairman of the South Carolina Bar Committee on the Unauthorized Practice of Law (UPL). As such, I was called to testify in a case where a gentleman was charged under the UPL statute. One of his defenses was that he had a contract to represent his client, and that the UPL Statute impaired his "right to contract." Thus, he claimed, the UPL statute was unconstitutional.

The man represented himself, and as such was given plenty of "latitude" during the trial. While I was testifying, he asked me this: "Sir, isn't it true that as a citizen of South Carolina I am free to contract with anyone for any act upon which we together agree?" My answer of "No," seemed to surprise him. "It isn't," he replied? "No sir, it isn't. For example, you cannot contract for an act which is illegal." He continued on, pointing to the bailiff and said "So, if I contract with this man to go out and collect cans for me, and we both honor the contract, that wouldn't be OK?" Retort – "There is nothing illegal about picking up cans." He continued: "So, how is that different from me contracting with my client to represent him in a legal matter." Response: "Because it is illegal to practice law in South Carolina if you are not a licensed lawyer, and you sir, are not a licensed lawyer." The man really did not understand the difference. He later claimed the SC Bar was a business, and as such had a monopoly on the practice of law. "A for effort," but he didn't get too far.

Lastly, there are many types of contracts, sometimes depending on state law, which would be for illegal acts and are therefore void. "Contracts" for sex are illegal in most places in the U.S. Contracts to sell people and body parts are also mostly illegal, as are contracts to sell illegal drugs and those designed to restrict housing for the poor. To defend by saying "But I had a really good reason," usually does not make a difference.

We often share "Friday Material" on the ListServ, and more often on the Water Cooler. I ran across a sentimental reminder of such an occasion recently, as I reviewed the archives in preparing another column. The ListServ to an extent, and the Water Cooler more often, are ways we communicate with each other across this big country on a wide range of personal and social issues. I ran across an example of our "human side," in discovering the following note I sent to the ListServ: (partial transmission)

"Folks - Please excuse the cross-post, but I know that many are interested in the situation:

Ladies and gentlemen: I have just received a phone call from Deborah Bailey. Brad passed away this morning at 9:31 a.m. (11:31 a.m. EST, I suppose) He had slipped into a coma and went very peacefully. As you can imagine, Deborah is broken up, and asked that I send out news to the IMLA circuit."

That one note alone resulted in one of the longest "email strings" in my archives. Many of us knew Brad Bailey personally, and even more knew him socially and professionally. He was a frequent contributor on the ListServ and Water Cooler, and his wisdom and insight were widely known and respected. It is fortunate that we were all able to share our thoughts across the miles to remember such a fine man. Let's please continue to use the ListServ to the extent allowable and then, of course the Water Cooler, to remind ourselves that there are more important things in life than work. We can all strengthen our common bond as municipal attorneys through the sharing and exchange of thoughts and ideas that are outside the realm of legal work. We are all in this game (life) together.....

I hope as many of you as possible can attend the IMLA Annual Convention this fall in San Diego. As usual, I will be planning the annual Water Cooler Reunion. This will be the fifth such event. They have grown each year at the annual conference. Last year was a great time at the Hofbrau Haus in Las Vegas. Rumor has it that if you were there you got to see various IMLA members "paddled" by one of the German waitresses. And, Rick from Pawn Stars dropped by too!

The prosecution rests, your honor...

Have A Job Position That You Need To Fill?



Use IMLA's job board to reach top quality candidates.
Take advantage of our 20% discount until August 31,2016! promo code: 5BA7HYK2
. Visit www.imla.org and click on the job board tab.

Phone: 202.466.5424
Fax: 202. 785.0152
E-mail: info@imla.org
Website: www.imla.org

7910 Woodmont Avenue
Suite 1440
Bethesda, Maryland 20814

Federal Cont'd from page 22

tobacco products, however, preempt state and local requirements that are different from, or in addition to, the federal requirements.[20]

The FDA also indicates that during the notice and comment period, it notified State and local jurisdictions about the potential impact the new rule would have on their current requirements. At the end of the comment period, no state or local law was identified that would be preempted by the final rule.[21]

Notes
1. FDA Tobacco Deeming Rule, 90 Fed. Reg. 28,974 (May 10, 2016) (to be codified at 21 C.F.R. §§ 1100, 1140, and 1143).
2. Tobacco Act, Pub. L. 111-31, 123 Stat. 1776 (codified as 21 U.S.C. §§ 387 et. seq.).
3. *See* Soretta, Inc. v. FDA, 627 F.3d 891, 897-98 (D.C Cir. 2011).
4. Pub. L. 111-21 (codified as 21 U.S.C § 301).
5. 21 U.S.C. § 387.
6. FDCA § 201(rr) defines "tobacco product," as "any product made or derived from tobacco that is intended for human consumption, including any component, part, or accessory of a tobacco product." 21 US.C. § 321(rr).
7. 90 Fed. Reg. at 28,976.
8. *See* Sabrina Tavernise, *F.D.A. Imposes Rules for E-Cigarettes in a Landmark* Move, N.Y. Times, May 5, 2016, http://www.nytimes.com/2016/05/06/science/fda-rules-electronic-cigarettes.html.
9. 90 Fed. Reg. at 28,976. *See also* 21 U.S.C. § 387(g).
10. *See* Tavernise *supra* note 8.
11. 90 Fed. Reg. at 28,977.
12. Covered tobacco products now includes not only those which contain any tobacco or nicotine, but also those that contain any tobacco derivative. *See also* 21 C.F.R. § 1100.2.
13. 90 Fed. Reg. at 28,976.
14. § 1140.16(d)(1).
15. 478 U.S. 697, 706-07 (1986).
16. 90 Fed. Reg. at 28,986.
17. 674 F.3d 509, 541 (6th Cir. 2012).
18. 90 Fed. Reg. at 28,989.
19. 90 Fed. Reg. at 28,989.
20. § 387(a)(2)(A).
21. 90 Fed. Reg. at 28989.

Inside Canada Cont'd from page 25

interpretation was owed deference and therefore, reinstated the arbitrator's award and allowed the appeal.

City Successful in Proving Civil Contempt

Langford (City) v. Dos Reis, 2016 BCCA 201 (CanLII) http://canlii.ca/t/gr8pn

The City of Langford ("City") successfully obtained an order from the court, requiring Dos Reis ("Respondent") to remove a building from her property as it was in violation of the City's zoning bylaw. The order required the Respondent to remove the building within 60 days, which the Respondent failed to do. The City agreed to multiple extensions between June and November 2015. In its final attempt for compliance, the City advised the Respondent in January 2016 that it would be proceeding with the application if the building was not removed. In the interim period the Respondent attempted to bring the building into compliance instead of removing the building. Ultimately the City filed a contempt application in February 2016.

HELD: The declaration of contempt was granted.

DISCUSSION: The respondent began by arguing that this issue should have been brought forward by the City in the Supreme Court. The Court of Appeal disagreed relying on *Peel Financial Holdings Ltd. v. Western Delta Lands Partnership*, 2003 BCCA 551 (CanLII) which stated that,

The court and a justice have the same powers as the Supreme Court in relation to matters of contempt of court.

After determining that the Court of Appeal was an appropriate forum to determine civil contempt, the Court outlined the three elements of civil contempt as found in the Supreme Court of Canada decision of *Carey v. Laiken*, 2015 SCC 17 (CanLII),

The first element is that the order alleged to have been breached "must state clearly and unequivocally what should and should not be done." The second element is that the party alleged to have breached the order must have had actual knowledge of it. Finally, the party allegedly in breach must have intentionally done the act that the order prohibits or intentionally failed to do the act that the order compels.

As the majority of the facts of this case were undisputed, the Court determined that the City was able to prove all three elements of civil contempt beyond a reasonable doubt.

Second Look Cont'd from page 23

dislike the "subject to objections" formulation because it leaves ambiguity about whether the objection is being waived or whether any responsive materials are being withheld – and the courts are treating the language as a waiver of the objections.[3] So make it clear that you are withholding materials that are covered by the objection. Instead, for objections based on proportionality, overbreadth, or availability, the responding party can indicate what data platforms or repositories were searched in response to the RFP, which the drafters' notes on the 2015 amendments accept as sufficient indication that items are being withheld because anything responsive that is not where a search was made will not be produced.[4]

When objecting to overly broad or ambiguous definitions for RFPs, where possible try to provide an alternative reasonable scope of definition or request, and produce nonprivileged documents responsive to the narrowed RFP. Courts love this and you will appear to be the soul of reasonableness. Here is where production "subject to" an objection can be property used. But carefully explain what you are doing and why your approach is not the typical defective reliance of "subject to" RFP responses.

Other than documents being withheld on the grounds of privilege or trial preparation, there is no obligation to list withheld documents, so object to any instruction that requires that you do so. Of course, a court can always order you to prepare and file such a list – consider asking for leave to file the list ex parte or for a nondisclosure order if you receive such an order and think the list will disclose core work product or confidential information. Among the grounds for objecting to RFP instructions that purport to require a list of withheld documents (other than privileged documents or documents protected by agreement or court order) are:

Attorney-Work Product: The list of excluded documents reflects the litigator's thought processes respecting the case;

Beyond the Scope of Permissible Discovery. Fed. R. Civ. P. 26(b)(2) has two prongs: proportionality and relevance. A list of withheld documents by definition solicits information that is not, in

the producing lawyer's view, relevant. So object by stating to the effect that "The instruction seeks documents and information outside the permissible scope of pretrial discovery by seeking matter that is not relevant to any party's claim or defense." Fed. R. Civ. P. 26I(b)(2).

Improper RFP Request: An RFP can seek the production of documents, but depositions and interrogatories are the only authorized means for obtaining narrative information such as lists or descriptions (except as to privilege logs (Fed. R. Civ. P. 26(b)(5)(A)) and lists of platforms not searched for responsive information (*See* 2015 Committee Notes on Rule 34(b)(2)(C) ("An objection that states the limits that have controlled the search for responsive and relevant materials qualifies as a statement that the materials have been 'withheld.')).")

Object to demands that a privilege log must contain information more detailed than what is sufficient to "describe the nature of the documents, communications, or tangible things not produced or disclosed—and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim." Fed. R. Civ. P. 26(b)(5)(A)(ii). Of course the log also must assert the specific privileges or trial preparation grounds on which you base withholding. Fed. R. Civ. P. 26(b)(5)(A)(i). In your objection state what information you will include (usually, identify the privilege(s); from/to/cc and who present, if live communication); subject of communication without disclosing privileged information; and date).

Here are some specific form Objections to Requests for Production:

Defendant objects to the instruction(s) requiring Defendant to allow Plaintiff to inspect documents and ESI described by the RFPs [specific citation(s) to each such instruction] and instead will produce copies of documents and ESI in lieu of permitting inspection, Fed. R. Civ. P. 34(b)(2)(B), of documents and ESI that Defendant does not withhold under the objections and privilege claims asserted below, *see* Fed. R. Civ. P. 34(b)(2)(C),[5] or that might reside only in locations that Defendant does not search based on the objections asserted below. *See* R. 34 Committee Notes on Rules–2015 Amendment (last paragraph).[6]

Defendant objects to the definitions of "City of AAA," "You and Your" and "BBBB" (Definition Nos. ___, ___, and ___ in the Requests for Production ("RFP") on the grounds that:

By including the terms "purported [apparent] agents, officers, and employees," the definition renders each RFP that incorporates any of these definitions too broad, vague and ambiguous to permit response because Defendant cannot know and cannot reasonably be required to determine whether any specific individual or entity might purport [have appeared] to be an agent of Defendant.

The terms "successors" and "affiliates" are overly broad and demonstrates that any RFP that includes either of those terms was not tailored to the facts of the instant case, because as a matter of law in the context of this litigation a city, and Defendant in particular, has no "successors" or "affiliates."

Therefore, Defendant will use the terms "City of XXX," "Defendant," "You," and "Your(s)" to mean only "City of XXX" in conducting searches for documents and ESI responsive to any RFP, and will not search for any of the terms "agents, officers, employees, successors, or affiliates" when is searches for the name of the Defendant. These are "limits that [control] the search for responsive and relevant materials." *See* R. 34 Committee Notes on Rules–2015 Amendment (last paragraph). However, Defendant will apply the concepts of Fed. R. Evid. 801(d)(2) in determining whether any statement by an employee or other agent is a statement attributable to Defendant in identifying responsive documents and ESI.[7]

This objection number 2 is hereinafter termed the "Definition Objection."[8]

Defendant objects to Instruction No. ___, which purports to require Defendant to produce electronically stored information ("ESI") either "as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request," on the grounds that this instruction purports to expand the obligations of Defendant for production beyond the requirement of the Rules. Fed. R. Civ. P. Rule 34(b)(2)(E)(i) requires a producing party to produce "documents" that way, but there is no corresponding requirement to produce ESI under either such organizational protocol. The Defendant is producing ESI in [format] [which is searchable or which was the format requested by Plaintiff] with metadata or a separate report indicting the original location of each electronic file. This provides substantially the same information as if produced as organized in the usual course of Defendant's business.

Defendant objects to Definition No. ___ defining the term "identify" [Instruction No. __, purporting to set forth the items to be included when identifying a document, person, or thing] on the grounds that such [definition/instruction] improperly attempts to expand the duties of Defendant beyond its duties in connection with production as set forth in the Fed. R. Civ. P. Defendant will identify documents withheld under claim of privilege or as trial preparation materials "in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim" Fed. R. Civ. P. 34(b)(2)(C). This may or may not include some or all of the elements purportedly required by the objected-to [definition/instruction].

Defendant objects to this RFP No. ___ [set out the RFP in full and immediately after quoting it to assert objections and then responses to the RFP] [to the extent that said RFP would require Defendant to retrieve, review, and produce ESI from the period January 1, 1999, through December 31, 2014 (the "Time Period"), that is archived only on disaster recovery tapes on the grounds that the request is disproportionate to the needs of the case within the meaning of Fed. R. Civ. P. 26(b)(1) and therefore beyond the proper scope of pretrial discovery, and on the further ground that such ESI is "not reasonably accessible because of undue burden or cost" within the meaning of Fed. R. Civ. P. 26(b)(2)(B), in that::

Plaintiff alleges that it has been damaged by "approximately $300,000." Third Amended Complaint ("Complaint"), para. 44.

The attached declaration under penalty of perjury under 28 U.S.C. § 1746 from Joe Blitz, Defendant's Chief Information Officer ("CIO") (the "Blitz Declaration"; Exhibit 1) establishes that:

Blitz has been CIO for 10 years, is knowledgeable based on the education, training, and experience detailed in the Blitz Declaration on the processes and costs for storage and restoration of disaster recovery tapes

Second Look Cont'd from page 33

of the type used by Defendant and of the activities of his department;

that there are 342 reels of disaster recovery tapes that each might include ESI from the Time Period; that there is no way to determine whether any responsive ESI is on any reel without first restoring the entire contents of the tape on each reel into readable form; that until each reel's tape if fully restored, no portion of the tape is readable; that restoration of the contents of each reel would take approximately 24 hours; that during the restoration of such tape a technician employed by the City would have to interrupt other important duties (enumerated in the Blitz Declaration) to monitor the tape to ensure the restoration is proceeding without damaging the tape; that the hardware used for such restoration (described in the Blitz Declaration) is the only method available in Defendant's City Hall for restoration of archived ESI; that if restoration of other ESI became necessary during restoration of the ESI for this litigation, vital governmental functions could be interrupted or impeded, but that it is impossible to know now what the nature of such functions might be; that if restoration of this litigation had to be interrupted to perform other governmental functions, interruption of the restoration in progress likely would irretrievably corrupt or delete ESI on the tape being restored or require completion of the restoration in progress, which could delay performance of governmental functions for up to 24 hours depending on the progress of the tape restoration in question; that the Defendant's restoration hardware (described in the Blitz Declaration) is so old that it has become difficult to find a vendor who could perform the restoration off-site for this litigation, and that after inquiry about prices from several such vendors (detailed in the Blitz Declaration) such vendor would charge no less than $60 per hour for restoration and would not indemnify Defendant for possible loss of data; and that Defendant rotates the 342 disaster recovery tapes and incrementally backs up disaster recovery data on a new tape each week; that because nobody knows what data is on which tape it would be useless to preserve only one or some of the tapes without preserving all of them; that if required to preserve all the tapes, the Defendant would have to spend $50 for each tape to replace each; that it would not be prudent to work with fewer than 342 tapes in order to minimize risk of losing key ESI; that taking the existing tapes out of rotation would pose a substantial risk of corrupting or losing critical data; but that if forced to do so the City would incur a replacement tape cost of at least $17,100 in addition to the incalculable risk of losing irreplaceable data.

Much of the substantive information that might subsist on Defendant's Disaster Recovery Tapes probably exists on paper documents or among ESI that Defendant is searching is response to RFP No. __. By the nature of things, it is impossible to be sure that there is no unique, responsive ESI on those tapes, but only the unduly burdensome recovery process described above would allow anyone to determine that issue. The attached declaration under penalty of perjury under 28 U.S.C. § 1746 of Josephine Ritz, the Defendant's Director of _____ (the "Ritz Declaration"; Exhibit 2) establishes that her department's current and former personnel were the individual Defendant's employees most directly involved in the events related to the Complaint (without admitting that any specific fact alleged in the Complaint is accurate); that she has been in charge of that department for 12 years; that although there is no policy in this regard, in her experience, the personnel in her department rarely delete email from their inboxes or outboxes; and that although there is no policy to image or otherwise preserve emails of employees when they leave the department, most of the emails of former employees are usually preserved because copies of their emails were sent to or from, or copied to other employees who have not left the department; and that although there is no policy requiring them to do so, employees, including Ritz, often print out and file in paper format, what they believe to be significant emails related to Defendant business.

[State what you are are going to provide. Save cost sharing request for countermotion to motion to compel].

Notes

1. However, a party can seek protection from unduly burdensome RFPs for paper documents (and ESI) under Fed. R. Civ. P. 26(b)(1) (specific objection showing how an RFP is disproportionate to the needs of the case) or a motion for protective order based on disproportionality, Fed. R. Civ. P. 26(b)(2)(C)(iii), or on the grounds that the RFP "is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive," Fed. R. Civ. P. 26(b)(2)(C)(i), or where "the party seeking discovery has had ample opportunity to obtain the information by discovery in the action." Fed. R. Civ. P. 26(b)(2)(C)(iii). On motion the court could order cost shifting, among other remedies.

2. *See* Johnson v. Kraft Foods N. Am., Inc., 236 F.R.D. 535, 538 (D. Kan. 2006).

3. *See, e.g.*, "An objection and answer preserves nothing and serves only to waste the time and resources of both the parties and the court. Answering discovery requests 'subject to' objections is 'manifestly confusing (at best) and misleading (at worse), and has no basis at all in the Federal Rules of Civil Procedure.'" The court could find "whenever [defendant's] answer accompanies an objection, the objection is deemed waived and the answer, if responsive, stands." Nonetheless, the court will address the validity of defendant's objections. Great Plains Ventures, Inc. v. Liberty Mut. Fire Ins. Co., 14-1136-JAR, 2015 WL 404977, at *2 (D. Kan. Jan. 29, 2015) (footnotes omitted), *review denied*, 14-1136-JAR-JPO, 2015 WL 1978356 (D. Kan. May 1, 2015). However, not all courts agree. *See* Whitley v. McClain, 4:13-CV-994 (CEJ, 2014 WL 1400178, at *1 (E.D. Mo. Apr. 10, 2014) (production "subject to objections" permitted by rules so long as nature of objection clear).

4. "The producing party does not need to provide a detailed description or log of all documents withheld, but does need to alert other parties to the fact that documents have been withheld and thereby facilitate an informed discussion of the objection. *An objection that states the limits that have controlled the search for responsive and relevant*

materials qualifies as a statement that the materials have been "withheld." R. 34 Committee Notes on Rules–2015 Amendment (last paragraph) (emphasis added).

5. "An objection must state whether any responsive materials are being withheld on the basis of that objection. An objection to part of a request must specify the part and permit inspection of the rest." FED. R. CIV. P. 24(b)(2)(C). Therefore, in objecting to each RFP as to which Defendant withholds documents or ESI, the Defendant should either state that documents are being withheld pursuant to this objection or state the fact that the Defendant's search for responsive documents and ESI will be limited to conform to the objection (the "limits that have controlled the search" *See* infra note 6 below). Do not rely on the general objection alone.

6. "The producing party does not need to provide a detailed description or log of all documents withheld, but does need to alert other parties to the fact that documents have been withheld and thereby facilitate an informed discussion of the objection. *An objection that states the limits that have controlled the search for responsive and relevant materials qualifies as a statement that the materials have been "withheld." See* R. 34 Committee Notes on Rules–2015 Amendment (last paragraph) (emphasis added). In order to

7. FED. R. EVID. 801(d)(2) treats as statements of a party (and thus not hearsay) certain types of extrajudicial statements including statements that "the party manifested that it adopted or believed to be true;" that were "made by a person whom the party authorized to make a statement on the subject;" that were "made by the party's agent or employee on a matter within the scope of that relationship and while it existed;" or that were "made by the party's coconspirator during and in furtherance of the conspiracy."

8. It is not sufficient to make the objection here. It needs to be iterated as an objection to each RFP to which the objection applies; in this situation, that likely will be each RFP. Therefore, objections to each RFP that incorporates the terms objected to should include a statement such as: "Defendant objects to this RFP on the grounds of the 'Definition Objection' and will limit the scope of its search as therein stated. "

Amicus Continued from page 29

used was excessive and because the City conceded that the use of force involved was in conformance with its "policy," summary judgment in favor of the City was therefore inappropriate.

In determining whether summary judgment was appropriate, the Ninth Circuit applied the *Graham* test to the facts in order to determine if there was a constitutional deprivation. In terms of the nature and quality of the intrusion, the Ninth Circuit reasoned that although Lowry's injuries were relatively minor, the district court erred on this factor by focusing solely on the amount of force used against her. Instead, the Ninth Circuit indicated that the court must look not only at the amount of force, but the type of force used and the *potential* harm it could cause. Because dog bites can be fatal, the court reasoned that the intrusion on Lowry's Fourth Amendment rights were severe.

The Ninth Circuit then brushed aside the City's countervailing interests under *Graham*, concluding that a jury could find that any belief that Lowry posed an immediate threat to the officers when they released the dog was unjustified. On this point, the Ninth Circuit analyzed the facts from Lowry's perspective, instead of from the officers' perspective (a point the dissent emphasizes) – i.e., that she was fast asleep on the couch, did not engage in threatening behavior, or do anything other than lay quietly. In terms of the severity of the crime, the Ninth Circuit concluded that although burglary *can* be dangerous, it is not an inherently dangerous crime.

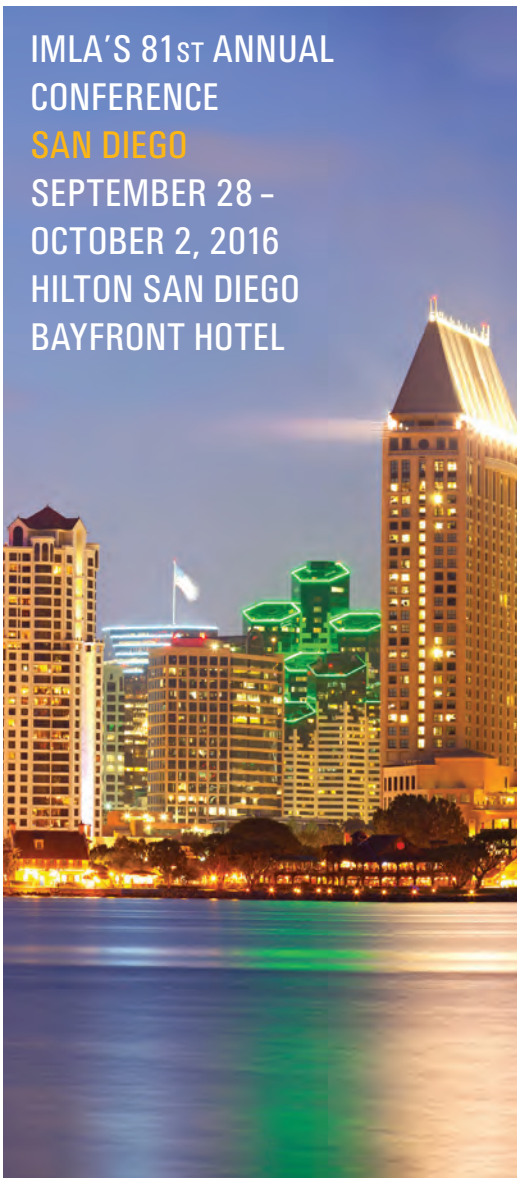
Although the district court concluded that the fact that the officers issued a warning weighed in favor of finding the use of force was reasonable, the Ninth Circuit concluded that this factor is accorded little weight because Lowry did not hear these warnings (again looking at the facts from Lowry's perspective). The Ninth Circuit also concluded that it would have been less intrusive to keep the dog on leash and therefore the fact that the dog was off leash militated against a finding that the force was reasonable.

Turning to the City's liability, the Ninth Circuit concluded that the City was liable under *Monell* due to its "bite and hold" policy as that policy was the "moving force" behind Lowry's injury. However, no formal policy exists and the Ninth Circuit failed to conduct a proper *Monell* analysis on a custom or practice claim.

The dissent criticizes the majority opinion for failing to evaluate the facts from the perspective of a reasonable officer on the scene and instead focusing on the facts from Lowry's perspective. The dissent also notes that the Ninth Circuit has "never held that the use of a police dog is categorically 'severe'..."

IMLA's amicus brief focused on the practical implications of the Ninth Circuit's decision and the limitations it would impose on police officers' ability to use police dogs. The brief also explains how police dogs are used by police officers and that they should be seen as a law enforcement tool, and not simply a weapon, like a gun, that is categorically a severe use of force.

To learn more about IMLA's amicus program, please visit our website at http://www.imla.org/legal-advocacy or contact Amanda Kellar at akellar@imla.org.



International Municipal
Lawyers Association
7910 Woodmont Avenue
Suite 1440
Bethesda, MD 20814

Nonprofit Organization
U.S. Postage
PAID
WEST

Codification Services
powered by MunicodeNEXT
municode LEGAL

- Online hosting
- Supplementation
- Codification
- enCodePlus Zoning Solutions

Government Websites
powered by aHa! Consulting
municode WEB

- Stunning design
- Easy for citizens and staff
- Outstanding customer support
- Rich suite of features

Online Payments
powered by Revalocity
municode PAY

- Reduce costs
- Improve operational efficiency
- Streamline all payment processing
- Traditional bill printing



Municode has proudly served America's municipalities for over 65 years.

We've done so with a tradition of providing outstanding service and cutting edge solutions for the future. That's how we fulfill our committment to helping our country's towns, cities, and villages realize their full potential while serving their citizens proudly.

municode
Connecting you and your citizens

Talk to us today
800·262·2633
municode.com