



# INTELNET *News*

Official Newsletter of the  
International Intelligence Network, Ltd.

*Intellenetwork.org*

*Spring 2018*



## *In this issue . . .*

### **PETER'S POSTING**

*By Peter Psarouthakis*.....2

**MEMBER NEWS**.....3

**"GENEALOGY'S IMPACT ON THE ANONYMITY OF ASSISTED REPRODUCTION"** *By Debra Allen* .....4

**"WHAT ARE THE BENEFITS OF DNA TESTING?"**  
*By Debra Allen* .....5

**"WHAT ABOUT THE EUROPEAN UNION'S GENERAL**

### **DATA PROTECTION REGULATION"**

*By Nicole Bocra Gray* .....6

**ISPLA REPORT** *by Bruce Hulme*.....10

**Tech Companies Face Congress  
Independent Contractor vs. Employee**

**The EU's GDPR**

**Police Use of Force**

**IASIR CONFERENCE 2018** .....15

Copyright 2018, International Intelligence Network. All rights reserved. Articles are on the authority of the author. Nothing herein should be construed as legal advice without consulting the appropriate legal authority.

# Peter's Posting

by

**Peter Psarouthakis**  
**Executive Director, Intellenet**



**Dear Intellenet Members:**

**At this year's conference we provided scholarships to three deserving young students. See below for the names of these special individuals.**

This year's annual conference has now concluded. What an amazing conference it was, as 111 attendees arrived in Aruba and enjoyed learning, networking and of course the sun and beach. George Michael Newman once again put on a great educational program with very diverse international speakers and topics. Thank you also to our new education director, Jeff Stein, for helping Michael this year. Our conference chairman Ed Spicer put on one great conference as everyone who attended can attest to. These three individuals spend countless hours of their own unpaid time to ensure that the conference is a success. Thank you so much for your efforts for our association.

This year for the first time ever our association founder, Jim Carino, was not able to attend the conference. That did not stop him from participating. On the opening day of the conference we were able to Skype Jim in on the big screen to welcome and address the attendees to everyone's delight. Jim was also able to use Skype and participate in our board of directors meeting. Jim assures us that he will be attending next year's conference in person.

Congratulations to the following two members who received awards this year. The Lifetime Membership Award

went to Bill De Genaro and the Brad Penny Special Recognition Award went to Ed Spicer. Both are extremely deserving. Well done, Bill and Ed!

Due to members generous contributions we were able to provide three educational scholarships again this year to very deserving young students. This year's scholarships were awarded to:

- Avery Gray (Nicole Bocra)
- Blake Ocampo (Sandra Stibbards)
- Ayla DeFatta (Jerry DeFatta)

Our auction to support the scholarship fund was a huge success this year. A big thank you to Remi Kalacyan for running the auction and making it a fun filled evening. Also, special thanks are offered to Marion Spicer, Tina Blanchette and Olga Cortez for running our registration table. Thank you to Peggy who works very hard for all members throughout the year and supports our conferences with many hours of administrative duties.



The 2019 conference is being planned and an announcement will be made very soon. Have a great summer!

As always you can reach me at [peter@ewiassociates.com](mailto:peter@ewiassociates.com).



# Member News

## Welcome New Members ...

Shahid AKHTAR—PAKISTAN/DUBAI

Osman ALI MALIK — PAKISTAN/DUBAI

(Shahid and Osman replace the late Rashid Ali Malik)

Debra ALLEN — Lake Havasu City, AZ

Carolina BETTERCOURT— Lisbon, PORTUGAL

Suhail BUDDHA — Mumbai, INDIA

Tom CASHIO — New Orleans, Baton Rouge, LA

Efrat COHEN — St. Louis, MO

Tom FISCHER — Milwaukee, WI

Kent HARRIS — Kansas City, MO

William (Bill) HICKMAN — Pittsburgh, PA

Greg HILL — Philadelphia, PA

Karl MILLIGAN — Annapolis, MD (reinstated)

David PARKER — Indianapolis, IN

David PIAZZA — Buenos Aires, ARGENTINA

Nicholis SMITH — Belmont, CA

These are our new members since we last published. To update your membership listing on the web, or in our Briefcase Roster, send info to [intellenet@intellenetwork.org](mailto:intellenet@intellenetwork.org).

## Congratulations, Jeff ...



**J**eff Stein and his company, ELPS, were honored recently with an award from the Office of the Secretary of Defense. Here's a note from Jeff:

"ELPS was honored and humbled in receiving recognition from the

Office of the Secretary of Defense, Employer Support of the Guard and Reserve as a Patriotic Employer for Contributing to National Security and Protecting Liberty and

Freedom by Supporting Employee Participation in America's National Guard and Reserve Force. I would like to thank our employee Basile Bishop for nominating ELPS for this recognition. ELPS strives to support and hire active and retired personnel from our armed forces. We thank all of our employees and those who have served and continue to serve our country! All Intellenet members can download our mobile app ... with great safety features. Here's the link: [ELPS Mobile App for iTunes](#), and the [ELPS Mobile App in Google Play](#)."

## Advanced Interviewing ...



**J**erry DeFatta and company are hosting a seminar this month. Jerry sends this note: "We are hosting a 2 day training session on Advanced Interviewing in Shreveport, LA later

this month (June 14, 15). This training will focus on identifying deception and obtaining admissions. This is great training for anyone who conducts interviews, such as HR staff, Auditors, and investigators of all types. Contact me if you have any questions or need additional information. We are offering group and government discounts."

For more details, see Jerry's post on [Facebook](#) or email Jerry at [jerry@defattapi.com](mailto:jerry@defattapi.com), or phone (318) 426-0199.



# Genealogy's Impact on the Anonymity of Assisted Reproduction

By Debra Allen

As a licensed private investigator and genetic genealogist, who uses DNA information on sites such as [www.23andme.com](http://www.23andme.com) and [www.ancestry.com](http://www.ancestry.com) to perform post adoption searches, heir searches, missing person searches, and skip tracing, I know the potential that these sites have for uncovering information that you may not have been looking for. It may also uncover the identity of someone that didn't think they would or could be identified.

While assisted reproduction produces children via a sperm or egg donation, it is far from clear how many children are conceived this way each year. Some estimate this number could be anywhere from 30,000 to 60,000 annually in the United States alone. In recent years, cases have hit the headlines where a donor unknowingly has hundreds of children, with a reported case of one donor fathering up to 150 offspring. Other cases have come up where a donor wasn't properly tested for various genetic diseases. Most of the time this is due to confidentiality agreements, where donors could opt never to be contacted. Other agreements limited contact to after the age of 18.

In this new age of DNA testing, with the ease and relatively low price to have testing done, can a donor truly remain anonymous? Should they remain anonymous? What role does the donation facility have to let potential donors know that it is getting easier than ever to be found, even if they don't test, but a relative does? And, what impact does this have on someone testing with one of these companies who was never told that the person who raised them was not their biological mother or father?

As the databases grow, the chances that a user might find a close genetic relative they didn't know they had, also grows. But none of the genetic testing companies

were designed to produce that result.

On the 23andMe website, the company has the following disclaimer:

"Looking at your genetic data might uncover information that some people find surprising. This information can be relatively benign. At other times, the information you learn can have profound implications for both you and your family. 23andMe cannot provide you with an ex-

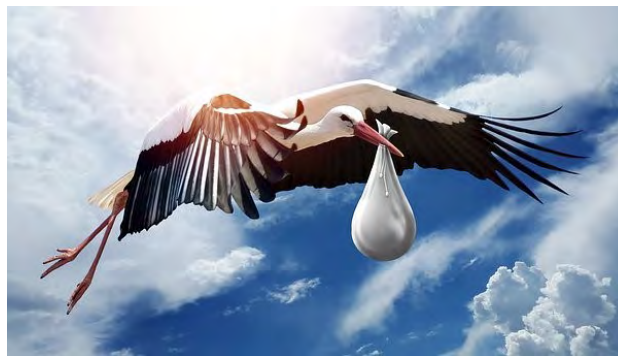
haustive list of all the unexpected things you might uncover during your genetic exploration ..."

And it goes on further to say, "In a similar way, genetic information can also reveal that someone you thought you were related to is not your biological relative. This happens most frequently in the case of paternity, where someone learns that their biological parent is not who they thought it was."

In 2005 researchers discovered that cases of paternity discrepancy, where a child is identified as being biological-

ly different than their purported mother or father, occurs between .8% to 30% in the population.<sup>1</sup>

I always recommend that the licensed private investigator act as an intermediary when contacting potential first family members. In the state of Arizona, I do post adoption work via the Confidential Intermediary program, through the Arizona Supreme Court. As part of my mandate, I always act as a go between when family members are found and have made this a standard practice in all potential reunion situations. This generally involves sending a letter from myself, explaining the situation, having the client write a letter to their family member, and including information about their rights to either share identifying or non-identifying (medical history) information. When donor parents or half-siblings agree to



**In this new age of DNA testing, with the ease and relatively low price to have testing done, can a donor truly remain anonymous?**

*Continued next page ...*

share identifying information, the rest is up to them, but most choose to get in contact right away, which I also encourage!

While it may be shocking, or a client may have known all along that they were the product of assisted reproduction, those who I have helped reconnect with their donor parents or half-siblings had very positive experiences.

<sup>1</sup> Citation: Bellis MA, Hughes K, Hughes S, et al, Measuring paternal discrepancy and its public health

consequences, *Journal of Epidemiology & Community Health* 2005;**59**:749-754.

*Debra is the owner of Allen Investigations in Havasu City, AZ. She is licensed as an investigator in Arizona and California, and she is certified as an adoption intermediary in Arizona. Debra can be reached at [debra@alleninv.com](mailto:debra@alleninv.com).*



## What Are the Benefits of DNA Testing? There May Be More Than You Know!



### WALMART VS. TARGET

**H**ow do Walmart and Target relate to DNA testing? If you are looking for something specific, and you thought you could get it at Walmart **OR** Target, but you weren't sure which, what would you do? Would you only shop at Walmart, and come away disappointed that they didn't have what you were looking for? Wouldn't you give Target a try to see if you could get what you wanted?

- Looking for familial ties is even more important, so why limit yourself to just one DNA testing company.
- There are many DNA testing companies out there, such as 23andme, Ancestry, and Family Tree, among others.
- The price of testing has come down dramatically over the years and there are numerous times throughout the year that test kits go on sale, you may be able to test less expensively than you think!
- Each company has its own proprietary or exclusive set of data.
- If you are serious about finding matches, testing with more than one company guarantees that your DNA is being matched with as many other people as possible. The major companies in this field each have millions of potential matches in their databases.

As a private investigator and genetic genealogist I encourage my clients to test. I not only encourage this for post-adoption searches, but genealogy can also provide leads on missing persons, heir searches, and skip tracing for difficult locates. Genealogy is evolving and can be an important tool for a private investigator. DNA testing and learning to how to use the information it provides adds to your tool box, to help you better serve your clients.



# WHAT ABOUT THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION?

## What does it mean in practical terms for those conducting due diligence in Europe?

*By Nicole Bocra Gray*

**On** May 25<sup>th</sup>, 2018, the *General Data Protection Regulation* went into effect throughout the European Union, including the UK.

Included in this regulation is the *right to be forgotten*, and the requirement that online service users under the age of 16 must have parental consent. Companies that are not in compliance with these new data security rules will face a fine of 4% of their annual revenue.

While companies like Google, Amazon and Facebook are working hard to come into compliance with these regulations – with some companies pulling products and features out of Europe entirely – there has been very little reported pushback against Europe's decision to tighten data security.

However useful these regulations are to protect data security, it has posed some new obstacles for investigators conducting due diligence in European countries. Many companies, organizations, and institutions have already tightened security standards in preparation for May 25<sup>th</sup>, especially universities and colleges.

So for anyone conducting due diligence in Europe or including European institutions, be aware that it is likely to take longer than expected, and be a much more involved process. The way companies and organizations deal with data access requests may vary and results will depend on how organizations interpret the new legislation.

Michael Ricks of UK investigations firm Enquire International Limited warns that universities in the UK are now demanding much more information with authorizing documentation before verifying credentials. Before, all that was needed was a general release from that applicant authorizing the release of academic information. Now, these requests are being rejected, as well as more detailed requests sent from personal rather than professional emails, especially emails sent from Gmail accounts.

Universities now require authorization from the applicant that are hand signed and specifically name the person or agency that the information can be released to. Some universities are even requiring multiple hand signed releases from the applicant be sent to different university departments, naming the agency or individual to whom information can be released as well as another separate request from the agency authorized to receive the data.

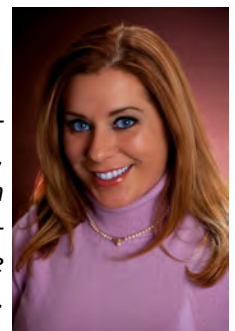
A German university recently denied a request for verification of educational qualifications for an applicant in the United States. The university stated that the information would only be released if the applicant came to the university in person to authorize the disclosure.

To avoid rejection, Ricks suggests always obtaining a detailed CV from the client or applicant and ensuring that any authority to release names the universities or organizations involved as well as the specific agencies, individuals, and organization that the information may be released to. This request should be submitted via the professional email address on letter-

head.

Even following these precautions does not guarantee you won't have to jump through extra hoops to obtain the data you need. These new regulations are open to interpretation by the institutions and their compliance departments and their introduction into policy is still very fresh. In the meantime, be sure to account for the extra time and effort due diligence in Europe will take.

*Nicole is the owner of Infinity Investigative Solutions in Arlington, Virginia, and a well-known speaker on open source intelligence and fraud investigations. She can be reached at [nicole@infinityinvestigative.com](mailto:nicole@infinityinvestigative.com).*





## ISPLA News for INTELLENET

By

**Bruce Hulme H. Hulme, CFE, BAI**

ISPLA Director of Government Affairs

**T**his article covers a wide range of hot topics including Facebook's Congressional hearing, its role with Cambridge Analytica, and potential litigation and regulation; *Capitol Forum's* recent article about Facebook possibly violating PI licensing laws; California's legal decision of note regarding independent contractor v. employee status; the EU's GDPR effective May 25, 2018, police use of force; and the May 7, 2018 filing with the SEC by Equifax regarding its 2017 PII security breach wherein 147 million U.S. consumers were victims of a hack.

### TOPICS OF CONCERN

#### TECH COMPANIES FACE CONGRESS:

**T**he U.S. Senate again sought testimony of Facebook, Google and Twitter executives on Facebook's data privacy practices, particularly with reference to its relationship to Cambridge Analytica, the British firm involved in the influencing of the 2016 presidential election. The Senate Judiciary Committee called Facebook's Chief Executive Mark Zuckerberg as a witness at its April hearing on the "future of data privacy and social media" --- to explore potential new "rules of the road" for the above mentioned tech companies. Cambridge had accessed names and "likes" of over 30 million users to create profiles on behalf of the Trump campaign.

#### Regulators Focus on Facebook ...

The Federal Trade Commission is investigating Facebook along with 37 State (and Territorial) Attorneys General at

last count, on how Facebook monitored, and how app developers utilized, data on Facebook users, and if Facebook had proper safeguards in place to prevent misuse. Facebook logged the phone call and instant messaging history of some Android smartphone users who had installed messaging app or a particular version of its main Facebook app. The call and text logging took place when smartphones on the Android operating system sync phone contacts with Messenger of Facebook Lite. Twitter users examining their Facebook data, saw the company logging the information and realized that they were sharing large amounts of data with Facebook each time they agreed to one of Facebook's privacy settings of feature requests. Facebook potentially violated its 2014 privacy agreement with the FTC. Expect the European Union to enter the fray as well.

#### Facebook May Be Violating State PI Licensing Laws ...

The *Capitol Forum* issued a report that "Facebook may be violating private Investigator licensing laws by collecting non-user data, according to interviewed experts" in a 3-page item of May 4, 2018. Included as experts interviewed by the publication were Peter Psarouthakis, Intelletnet's Executive Director and a founder of ISPLA, along with this writer. The article read in part:

*Facebook's collection of non-user information and its relationship with Cambridge Analytica sparked media attention and public outrage, with mainstream media popularizing the term "shadow profiles" to describe the portfolios of information Facebook collects about non-users. Facebook asserts that it has been collecting private data of non-users for safety and*

Continued next page ...

security reasons and to identify “identify bad actors,” according to recent public disclosures.

Legally, many states regulate the collection of information about an individual’s character, habits and whereabouts under state private investigator licensure law. Most experts of state private investigator law that we interviewed said that Facebook’s conduct likely violates state laws designed to regulate the private investigation industry.

For example, Michigan state law, which is similar to many other state laws, regulates companies and citizens who conduct an “investigation for the purpose of obtaining information with reference to the identity, habits, conduct...and whereabouts.”

Peter Psarouthakis, a Michigan private investigator and a co-author of some of the provisions of the Michigan Professional Investigator Licensing Act 285 of 1965, said that “if they [Facebook] are collecting this type of data then they are likely in violation of Professional Investigator Licensure Act.”

Private investigation activity without a license is subject to different punishment throughout the country, with penalties ranging from \$10,000 fines per infraction to multiple years of imprisonment. Beyond fines or potential imprisonment, if state law enforcers decide

to take action, Facebook could be faced with a decision to cease certain data collection activities or to come under regulation of state private investigator law.

Facebook is not the only company that may be violating states’ private investigator licensing laws. Google, Twitter, Pinterest and Mi-



### **... Facebook’s conduct likely violates state laws designed to regulate private investigators ...**

crosoft-owned LinkedIn are also collecting data from websites unaffiliated with their platforms through share buttons. Capitol Forum reached out to each of these companies for comment but did not receive a response by its publication date.

State laws for private investigators are mostly similar, but regulators and penalties vary. The article stated: “Psarouthakis, who also serves as executive director at the International Intelligence Network, said that most states’ laws are similar with some exceptions. The legal text often follows a template

adopted in majority of states when it comes to providing a definition of investigation business practices.”

Some experts suggested that Facebook might seek to define its activity in a way that would exempt it from state law.

Daniel Rowley, an employment attorney at Gilmore Magness Janisse, a Fresno-based law firm, suggested that Facebook may not qualify under California law as a private investigator because the company does not sell the information to 3rd parties. An April 18 blog post titled “Hard Questions: What Data Does Facebook Collect When I’m Not Using Facebook, and Why,” by David Baser, a product management director at Facebook, specifically stated “We don’t sell people’s data. Period.”

Facebook could also try to seek exemption from regulation under private investigator law by focusing on the intent behind its non-user data collection practices. During recent Congressional testimony, Mark Zuckerberg said that Facebook employees “collect data on people who are not signed up for Facebook for security purposes.”

Psarouthakis, however, explained that it is the collection of data, not the intent behind collecting the data, that matters to state investigator licensure law: “Intent is not important, but the actions performed are.”

There are also exemptions for businesses that collect information relat-



ed to human resources issues or other internal audits. But these exemptions likely do not apply to Facebook. Psarouthakis explained that Facebook employees “are conducting investigations that have nothing to do with internal mechanisms of their company.”

Of note, federal and state law enforcement, law firms, and some public utility companies are exempt from private investigative law in most states. The penalties for violations of state licensure laws vary significantly. In California, unlicensed activity would be considered an infraction, punishable by imprisonment. In Michigan, unlicensed activity is a felony, punishable by up to a 4-year imprisonment. In Texas, violation of chapter 1702 carries a civil penalty of \$10,000 per violation.

Some experts do not expect law enforcers to act. Some experts were skeptical that law enforcers would act, despite the likely violation of state law, saying that state regulators would be stepping into uncharted territory by investigating Facebook’s actions.

Speaking about the difficult issue of regulating internet companies, Billy Meeks, a president of Texas Association of Licensed Investigators, said that he didn’t think that the law was keeping up with the privacy concerns brought up by Facebook’s recent issues.

One industry executive who requested anonymity to speak freely

said that “enforcement in general would be unlikely; however, the GDPR (General Data Protection Regulation) passed in Europe, so, that might change the regulators’ approach.”

The above comment was mine, along



with numerous other ones that indicated the belief that Facebook's current practices would not necessitate the need for a private investigators license. I did stress that Facebook might undergo the wrath of the FTC for violating consumers' privacy rights and that some members of Congress were proposing measures to adopt the EU's GDPR here in the U.S. These comments, along with others, were not part of the *Capitol Forum* article. There are already positions taken by some members of Congress and Federal regulators that say Facebook and Google are media companies. Some officials state they are even utilities. Such descriptions alone would eliminate the requirement for falling under

state PI licensing statutes.

That said, the reporter, Ivan Zhykhariev-Kelly, also asked us whether Facebook is required to obtain a PI license after their recent public disclosure on the purposes of obtaining personal data of non-members. He ar-

gued that since Facebook collects data for security purposes, such data can identify person’s location and habits, also one’s character. These activities are, of course, defined in most state’s private investigator laws as the business of private investigation. He believed that Facebook and other companies who engage in such activities for security reasons ought to obtain PI licenses in each state they operate. I disagreed, as he asked that my opinion be based on a review of Facebook’s blog on the collection of data from non-users (those who are

not members of Facebook) through third-party websites. The Blog link outlined one of the reasons as safety and security on Facebook, which stated:

"There are three main ways in which Facebook uses the information we get from other websites and apps: providing our services to these sites or apps; improving **safety and security on Facebook**; and enhancing our own products and services." The blog also elaborated on what type of data is collected:

"We also use the information we receive from websites and apps to help protect the security of Facebook. For example, receiving data about the sites a particular browser has visited

can help us identify bad actors. If someone tries to log into your account using an IP address from a different country, we might ask some questions to verify it's you. Or if a browser has visited hundreds of sites in the last five minutes, that's a sign the device might be a bot. We'll ask them to prove they're a real person by completing additional security checks."

Mr. Zhykhariev-Kelly wrote me that "Facebook has been collecting and verifying IP addresses, **identifying "bad actors"**, also obtaining information on what websites one was visiting. These require licensure pursuant to Texas, Michigan, Arizona, New York, Alabama, [and] Indiana. Basically, the language is identical with few exceptions."

I advised him in a half hour telephone conversation numerous reasons why most likely Facebook and many other businesses would not require a license for ensuring security of their own businesses and consumers. In answer to his question: "Does this **exemption** apply to Facebook based on the info I provided?" My answer was 'No.' There are hundreds of social media platforms. Some post on their websites that they are "helping clients improve the customer experience, mitigate risks, and combat fraud." None are licensed as private investigators. In addition, marketing and direct mail companies are also acquiring vast amounts of data from many sources which they are evaluating for a wide range of purposes and they are not required to have a private investigator's license.

## INDEPENDENT CONTRACTOR VERSUS EMPLOYEE STATUS:

**A** question often asked of ISPLA by our investigative and security members concerns the determination of whether one is a subcontractor or an employee. Although the case cited below is from California, similar findings often arise in other jurisdictions. It should at least be carefully reviewed by our California members. Establishing that a worker in California is an independent contractor, as opposed to an employee, has always been difficult. Now the California Supreme Court has made it even harder.

In [\*Dynamex Operations West, Inc. v. Superior Court\*](#), the justices were asked to decide what test determines whether a worker is an employee under the California Industrial Welfare Commission Wage Orders. Under the new test, workers are presumed to be employees of a hiring business unless the business can satisfy three separate requirements to establish the worker's independent contractor status.

One cannot overstate the importance of this decision. The wage orders guarantee employees, among other things, minimum wages, maximum hours, overtime compensation, and meal and rest breaks. Independent contractors do not receive those protections. The court's broad interpretation of the meaning of "employee" under the wage orders will require many businesses that currently rely on independent contractors to reclassify workers as employees. This will not only impose substantial costs on

businesses that have relied on independent contractors, but also subject them to liability for not previously providing the wages, breaks, overtime, etc. that employees are entitled to.

### Facts ...

Two delivery drivers sued Dynamex, a courier and delivery company, alleging that it improperly classified them and similarly situated drivers as independent contractors. The drivers set their own schedules, decide what deliveries they'll make, and use their own vehicles. They are sometimes required to wear clothing with the Dynamex logo or place that logo on their vehicles. They are allowed to hire others to do the work and to work for other delivery companies or for themselves.

The trial court, in certifying the class of drivers, found that the wage orders define the term "employ" to mean "(a) exercise control over the worker's wages, hours, or working conditions, (b) suffer or permit work, or (c) to engage, thereby creating a common law employment relationship." The trial court rejected Dynamex's contention that the multifactor test of employees articulated in the California Supreme Court's 1989 decision in [\*S.G. Borello & Sons, Inc. v Department of Industrial Affairs\*](#) governed whether a worker was an employee or independent contractor under the California's wage orders. This is despite the fact that courts and administrative agencies in California have been using the test for decades. Even the Division of Labor Standards Enforcement, which enforces the Wage Orders,

states in its Enforcement Policies and Interpretations Manual that the *Borello* test applies.

Dynamex moved to decertify the class, arguing that two of the alternative definitions of “employ” discussed in another California Supreme Court case, *Martinez v Combs* (2010) 49 Cal.4th 35, 64, the “suffer or permit” and the “engage” tests, did not apply in this context. Both the trial court and the Court of Appeal rejected Dynamex’s argument. Dynamex filed a petition for review with the California Supreme Court, and the Court agreed to consider the issue.

The California Supreme Court agreed that the multi-factor *Borello* test, which focuses on the employer’s ability to control the manner and means of accomplishing the desired result, is not the only test to determine if a worker is an employee or an independent contractor. As it has done frequently of late, the court explained that it must interpret these protections broadly to protect workers from unscrupulous employers. The court also concluded that the new test it articulates provides greater clarity and consistency than a test that involves balancing multiple factors on a case-by-case basis.

### **The New Test ...**

The court adopted what is known as the “ABC test.” Workers are presumed to be employees of a hiring business unless the business can satisfy three separate requirements.

To establish that a worker is an inde-

pendent contractor under the wage orders, the business must show that: (A) the worker is free from the control and direction of the hiring business in connection with the performance of the work; (B) the worker performs work that is outside the usual course of the hiring entity’s business; and (C)



the worker is customarily engaged in an independently established trade, occupation, or business. The court, in its discretion, may start with any prong of three prongs of the test to resolve the question whether the workers are properly classified as independent contractors.

Prong “A” looks at whether the hiring business is able to control and direct what the worker does, both under the terms of the contract and in actual practice. The business need not control the exact manner or details of the work, as long as it maintains the level of control employers typically maintain over employees.

Under prong “B” the worker must be performing tasks outside the usual course of the hiring entity’s business.

This will be especially problematic for companies in the gig economy that rely heavily on independent contractors. No matter how much freedom those workers have to decide when to work, where to work, or what to do, if they are performing services in the usual course of the hiring company’s business, they will be deemed to be employees of the business. The Court used the examples of a retail business that hired an outside plumber to repair a leak and a clothing manufacturer that hired an at-home seamstress to make clothes from patterns and cloth supplied by the company. The outside plumber would be an independent contractor because he performed services outside the company’s usual course of business, but the seamstress would be an employee since the work performed is within the company’s usual course of business.

Under prong “C” the workers must be customarily engaged in an independently established trade, occupation, or business. The workers must have independently decided to go into business for themselves and, in doing so, independently accepted the burdens and benefits of self-employment. Further, it is not enough that the company has not prohibited a worker from engaging in such a business. To meet this standard, the individual should have taken the steps to establish and promote their individual business such as through incorporation or licensure, creating business cards, advertisement, or routinely offering their services to the public or to other potential customers. Unless the employ-

er can satisfy all three prongs, the worker is considered an employee.

### Key Takeaway ...

The new test is considerably broader and more inclusive than the *S.G. Borello & Sons* test which courts, agencies, and employers in California have relied on for years. Consequently, many businesses will need to revisit whether their workers qualify as independent contractors. If they do not, the businesses need to either modify the relationship or start providing the workers with the pay and treatment required by the wage orders. Since the decision only addresses the wage order requirements, different standards will apply in determining whether the workers are independent contractors for purposes such as workers' compensation and payroll taxes. The Labor and Employment attorneys at Fox Rothschild LLP are always available to help address these complicated issues.

This article is intended for general information purposes only and does not constitute legal advice. The reader should consult with knowledgeable legal counsel to determine how applicable laws apply to specific facts and situations. ISPLA is grateful to the employment law firm of Fox Rothschild, LLP and specifically to attorneys Charles O. Zulver, Jr. and Jeffrey D. Polsky.

## EUROPEAN UNION GENERAL DATA PROTECTION REGULATION (GDPR):

The enforcement date of the [EU General Data Protection Regulation](#) (GDPR) officially became effective on May 25, 2018 and will encumber any organization or business offering goods or services in the EU (whether or not a payment is involved) or that monitor the behavior of individuals in the EU, whether or not they have a presence in the EU. Regulatory requirements have ex-



panded data subject rights, and call for maintaining records of processing, documenting the legal basis for such processing, and complying with new security breach notification requirements. The commentary that follows is but a small part of what one may expect with this EU regulatory scheme. In addition, features of the GDPR are already being proposed by members of Congress aligned with privacy advocates in the U.S.

The GDPR replaces the previous [Data Protection Directive 95/46/EC](#) (the Directive) as the governing privacy regulation in the EU. While key principles of data privacy addressed in the Directive remain largely the same, there are some significant policy changes, and, as a result, a fair amount of uncertainty about how the regulation will be enforced. Where

the Directive included an obligation to notify supervisory authorities about an organization's processing activities, the GDPR allows organizations to document their own processing activities, determine if they are compliant with the specific requirements, identify and mitigate any risks created by their data use, and ultimately hold themselves accountable for compliance. The emphasis on accountability and record keeping is key. Organizations with a robust data governance program, that have a documented and considered approach to GDPR compliance, are less likely to undergo GDPR enforcement, wherein the highest fines (up to \$20 million or 4 percent of global annual turnover) are significant sanctions for noncompliance.

### Accountability for Risk-Based Approach ...

According to a March 2, 2018 item in the New York Law Journal by attorney Jessica B. Lee of Loeb & Loeb, "Article 5(2) of the GDPR introduces the accountability principle, which requires organizations that control the processing of personal data ("controllers") to demonstrate (read: document) compliance with the GDPR's principles relating to the processing of personal data (i.e., lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; and integrity and confidentiality). This notion of accountability is not new; it was included as a basic data protection principle in the [OECD Guidelines](#) in 1980 (and the most recent update in 2013) and has been incorporated in

various forms in other international privacy regulations. However, previous iterations of the accountability principle were centered on assigning responsibility or fault for failures in privacy compliance. Under the GDPR, accountability is recast as an obligation to establish a systematic and ongoing approach to privacy. In effect, it codifies the obligation to create a data governance program that incorporates the principle of privacy by design, using tools like privacy impact assessments to routinize data protection within an organization. More than just a mandate to create policy documents, the GDPR creates a regulatory environment under which privacy and data governance are forced to become a standard element of an organization's operations."

This principle of accountability must be viewed in the context of the GDPR's risk-based approach to privacy. Under Article 24 of the GDPR, controllers are required to assess the nature, scope, context and purpose of processing, and based on the risks presented: (1) implement appropriate technical and organizational measures to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR; and (2) review and update those measures where necessary. Organizations are directed to take into account "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons." The GDPR provides suggestions (although no mandates) for which

measures might be considered "appropriate to the risk." The pseudonymization and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and the creation of a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing will provide a good start for organizations to start mapping out their compliance efforts.

### Records of Processing ...

Under the Directive, organizations were obligated to notify and register processing activities with local DPAs. The GDPR eliminates this requirement and instead puts the burden on both controllers and processors to maintain an internal record of processing activities, which must be made available to DPAs upon request. These records must contain all of the following information: (1) the name and contact details of the controller and where applicable, the data protection office; (2) the purposes of the processing; (3) a description of the categories of data subjects and of the categories of personal data; (4) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations; (5) the transfers of personal data to a third country or an international organization, including the documentation of



Historically, [national data protection authorities](#) in Europe (DPAs) have recommended privacy impact assessments (PIAs), tools used to identify and mitigate privacy risks during the design-phase of a project, as an element of privacy by design. Under Article 35 of the GDPR, data protection impact assessments (DPIAs)—a more robust version of the PIA—are now mandatory when an organization is engaging in activities that pose a high risk to an individual's rights and freedoms. The DPIA presents an opportunity to demonstrate that safeguards have (hopefully) been integrated into an organization's data processing activities and that the risks presented by a processing activity have been sufficiently mitigated. While the risks analysis itself is largely left in the hands of each organization, determinations that are wildly off-base may not be defensible. However, if an organization can justify its position, relying on industry practice or other guidance, even if regulators ultimately determine that additional measures were required, it may be able to avoid significant fines. Notably, the failure to complete a DPIA itself could result in fines of up to 10 million Euros or up to 2 percent of the total worldwide turnover of the preceding year.

suitable safeguards; (6) the envisaged time limits for erasure of the different categories of data; and (7) a general description of the applied technical and organizational security measures. Where processing activities take place across a variety of disconnected business units, organizing these records may be challenging. Organizations will need to audit each of their business units and their corresponding systems and processes to determine their processing activities and consider moving to a more centralized system.

### Preparing for May 25th and Beyond ...

According to attorney Lee, organizations should be focused on creating the processes and documents that will reflect their GDPR compliance:

- Investigate and document the flow of data through your organization. Understand the sources of data the organization has control over, the systems or databases that data is stored in, the controls in place to protect that data, and how and when it's transmitted to third parties.
- Create records of processing and a process going forward for keeping those records up to date.
- Audit vendors and update agreements to include GDPR compliant provisions.
- Track the key requirements of the GDPR and document the data protection policies in place to address those obligations. Create a procedure for data breach response, data retention, and responding to data subject requests.

- Create a DPIA process—including a system to determine when a DPIA is needed and the team in charge of completion.

- Create a schedule and process to periodically audit the effectiveness of your data governance program.

- Conduct annual privacy training for employees.

Ms. Lee points out that although the process of preparing for the GDPR may be lengthy and expensive, "it may ultimately give information security and internal data governance teams the resources needed to more effectively and strategically manage an organization's data. And, as the GDPR creates affirmative obligations for controllers to vet third party vendors for compliance with the GDPR's obligations, being able to demonstrate compliance with the GDPR through a strong data governance program won't just be a required regulatory obligation; it may be a selling point that distinguishes you as an organization that is safe to do business with."

### POLICE USE OF FORCE — MOST SUSPECTS ARE NOT INJURED:

**I**SPLA is grateful for the following article by Denise-Marie Ordway, provided to us by *Journalist's Resource*:

Police officers rarely use force to apprehend and detain criminal suspects and, when they do, the majority of suspects are not injured, according to a new, [first-of-its-kind analysis](#) conducted by a research team comprised

mostly of medical doctors.

Fewer than 1 percent of arrests examined required the use of force, which can range from verbal commands, control holds and strikes with a closed fist to employing stun guns, chemical sprays, police dogs and firearms.

The research team, led by [William P. Bozeman](#) of the Wake Forest School of Medicine, found that 61 percent of suspects had no reported or observed injuries after officers used force during their arrest while 1.7 percent suffered moderate or severe injuries, including one death.

The findings appear to contradict public perceptions about [police use of force](#), which has faced increased scrutiny since the 2014 death of Michael Brown, a black teenager shot by a white officer in Ferguson, Missouri. In recent years, news reports of officers beating unarmed citizens have sparked outrage and questions about how police treat people of color.

For this study, the researchers examined more than 1 million calls for service made in 2011 and 2012 to police stations in three mid-sized cities: Mesa, Arizona; Shreveport, Louisiana; and Winston-Salem, North Carolina. Unlike previous studies, the researchers investigated the types of force used during each arrest and identified and classified all resulting injuries. A panel of five physicians reviewed all injuries considered moderate or severe to determine their final classification.

It's worth noting that the team did not look at suspects' race or ethnicity as a part of their study, published in

March 2018 in the peer-reviewed *Journal of Trauma and Acute Care Surgery*.

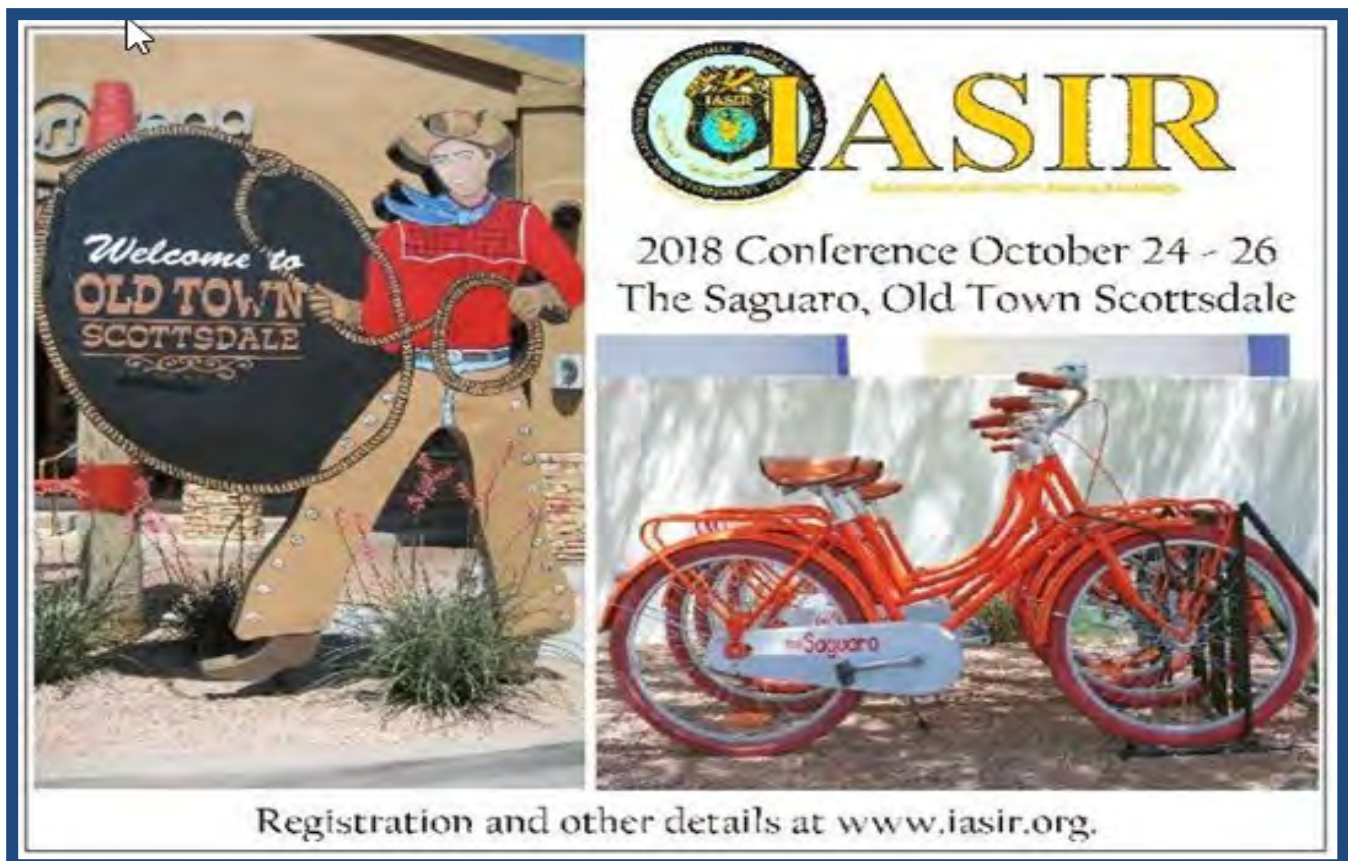
Some of the other key findings:

- When officers used force, they mostly used either physical force or stun guns. Fifty-one percent of the time, police used “unarmed physical force” — a category that includes control holds and joint manipulation as well as kicks, strikes with closed fists, knees or elbows and forcibly throwing someone to the ground. They used stun guns, commonly known by the brand name TASER, 36 percent of the time.
- Just over 6 percent of use of force incidents involved pepper spray. Another 3 percent involved police dogs.
- Firearms were used 0.4 percent of the time, representing a total of six incidents.
- Almost 40 percent of suspects suffered injuries as a result of police use of force. Of these, 37 percent had “mild” injuries — for example, abrasions and minor contusions. About 1 percent had “moderate” injuries such as bone fractures or a collapsed lung. Four people — 0.4 percent of suspects — suffered severe or life-threatening injuries.

- Firearms and police dogs were most likely to cause significant injuries. “While this is also consistent with common sense and previous reports, small sample size/rarity of use limit this to a preliminary conclusion. More detailed data collection at a national level is now being implemented and should confirm and clarify this risk.” Of the 355 suspects who were taken to the emergency room for a medical evaluation, 22 percent were hospitalized. Less than a quarter of those hospitalized had injuries related to officers’ use of force.

*For additional research on this topic, check out a longer research review on [police use of force](#). Also available are write-ups on [deaths in police custody](#) and how [body cameras](#) change the way officers interact with the public. *Journalist's Resource* is part of Harvard Kennedy School, Shorenstein Center on Media, Politics, and Public Policy and the Carnegie Knight Institute.*

Bruce can be reached at [brucehulme@yahoo.com](mailto:brucehulme@yahoo.com). Please consider donating to [ISPLA](#) to assist in its continuing mission.



The advertisement is enclosed in a blue border and is split into two main sections. The left section features a photograph of a cowboy statue in a red shirt and tan pants, holding a large black sign that reads "Welcome to OLD TOWN SCOTTSDALE". The right section features the IASIR logo, which includes a circular seal with a globe and the acronym "IASIR" in large, bold, yellow letters. Below the logo, the text reads "2018 Conference October 24 - 26 The Saguaro, Old Town Scottsdale". At the bottom of the right section is a photograph of several orange bicycles parked in a row. At the very bottom of the advertisement, the text "Registration and other details at [www.iasir.org](http://www.iasir.org)." is displayed.