PERSPECTIVES

SCHERER SMITH & KENNY LLP
THE STRENGTH OF PARTNERSHIP

140 Geary Street, Seventh Floor ▪ San Francisco, CA 94108-4635
Phone: (415) 433-1099 ▪ Fax: (415) 433-9434 ▪ www.sfcounsel.com

April 2018

Scherer Smith & Kenny LLP serves mid-sized and fast-growing entrepreneurial companies. From complex litigation to business, real estate, intellectual property and employment law, our team brings strategic thinking, pragmatism and intense dedication to our clients' success.

Data Breach!

While we hear these words seemingly every day (and may becoming immune to their effects), the ramifications for the companies that suffer the breach have only become more severe and onerous. As more and more companies collect valuable, and often very personal, data about their customers, the issue of data privacy and security is expanding far beyond companies that are focused solely on data aggregation. For example, clients that offer artistic apps, but collect data about the demographics of theirs users, or health and fitness apps that collect personal health data about their users, all must follow the privacy laws and practices.

The issue of data privacy and security comes up several ways for our clients. Some are the result of legislation, both within the U.S. and abroad (and often our U.S. based clients are surprised to learn that they may need to comply with EU based laws, for example), and others are best practices. This short article is meant to be an introduction to these areas, but is not meant to be a detailed summary. It won't discuss data security, which you should be very focused on from the outset, but focuses more on things you can do both now and if a breach occurs.

Privacy Policy

If you are collecting data (i.e. name, email address, IP address, cookies, demographics etc.) from your customers, you need a privacy policy in place. This is to request their consent, if needed (under statute or to comply with a third party service such as Google AdSense), and to explain what data you are collecting and how you'll be using and sharing it, if at all. Without this, you may, depending on the statute, be violating the law, and at a minimum, you are missing an opportunity to communicate with your clients in a way that is transparent. Doing so will create trust and

In This Issue

William Scherer

If you are a reader of the Partner Notes section of our *Perspectives* quarterly update, you know that each of our partners take turns writing

minimize opportunities in the future for someone to allege you are improperly collecting and using data.

Privacy is becoming more regulated in the U.S. and the EU recently passed the GDPR (General Data Protection Regulation) that established certain basic rights that individuals have regarding privacy. Monetary fines for failing to comply with these regulations or not properly responding to a breach situation can be huge (easily in the millions of dollars) so starting off on the right foot with a good privacy policy is a great way to start your protection from the beginning.

Basics that should be included in a privacy policy is your company's name, what information you are collecting, how you are collecting it and how you'll use it, whether is it optional or if opting-out is an option and how you are keeping their information secure. We often draft privacy policies for our clients or review existing ones to make sure they are appropriate for each client's individual situation.

Insurance

If you are collecting personal information, and definitely if you are collecting personal health information, we strongly recommend that you purchase cyber insurance. This insurance will help provide coverage if there is a breach and usually will cover attorney's fees, mitigation costs (breach notification, credit monitoring etc.) that may be mandated either under statute or in a contract with your customer or vendor. We recommend that you get as much as you can afford, as the cost for mitigation alone can be very expensive. For example, if you are holding 100,000 users' information and it costs $7.00 to notify and offer credit monitoring to each of them that is $700,000 in costs alone (excluding lawsuits, fines, legal fees etc.).

Recommendations

After you have a privacy policy and insurance in place, if possible, you should set out an "incident response plan" that involves all the relevant people (management, IT, legal, insurance, PR etc.) who be involved if there is a breach. We recommend against having it be too "aspirational". You don't want to later produce a plan only to have that plan attacked because you never followed it. It should be as simple as possible. Have all key phone numbers and contact people in place and know what order you'll call each person in the chain. It's best, ideally, to have those accessible offline so that if your entire system is compromised and you cannot get into your database (denial of service attack, ransom ware etc.) you can still contact the key individuals.

You should also review your vendors each year to figure out what type of security risk they represent as far as security of your data. Are they holding it in an unsecure manner? Do they have access to your critical systems but don't have processes in place to make sure only authorized individuals are accessing your system?

Ideally you'll also have internal policies about how people should communicate if a breach occurs. You'll need to decide who is authorized to speak to the press, customers and vendors and if so, through what channels.

If you do suffer a breach, the first thing to do is to take a deep breath and not panic. This is critical, as panicking and rushing a response can be

them. The essential purpose is to provide a personal take on our lives as lawyers, to share our thoughts and beliefs, and what we do outside of our professional lives. It is intended to be light and thoughtful.

This issue – obviously – is my turn. In all candor I have been struggling to find a topic to discuss, or even to riff on. In fact, my challenges delayed publication of this edition. As a lawyer, my lack of ideas and the desire or ability to convey them is not typically an issue. And yet, here I was, walking around the office with this empty thought bubble over my head for several weeks. And I also couldn't figure out why I could not think of a subject. Finally, it hit me.

Whatever your politics, point of view, geography, or upbringing, I think it's safe to say the issues that are most

disastrous to your business. Each day is different than the one before and how you feel in the first few hours will be different than a day or two later. This isn't to say you don't need to act quickly, which you will since some statutes, such as the GDPR, or contractual arrangements require notice within a short time frame (often 48-72 hours). However, before doing so, take the time to contact the right people to help you figure out the best way to proceed.

If you have insurance you'll want to consider tendering it to your insurance company as soon as possible, as often they won't pay for legal fees incurred before you do so.

It's also important to recognize that not every "breach" will result in a notice obligation or liability. Only after analyzing what was accessed, how it was accessed, whether any data taken, destroyed etc., will you know what you need to do.

Finally, make sure to figure out quickly whether it is a live leak (*i.e.* ongoing) or if it occurred six months ago. How you will respond will be very different depending on the answer to this critical question.

In sum, there are steps you can take now to minimize your exposure, comply with the law, build client trust and reduce your cost, stress and anxiety in the future if a breach occurs. Remember that many companies have gone through this and come out the other side and with the proper planning and response you will to if ever faced with a breach.

Please contact Heather Sapp at (hgs@sfcounsel.com) or Brandon Smith at (bds@sfcounsel.com) for more information on privacy policies and data privacy.

- Written by Brandon Smith

Instructive Administrative Exemption Ruling for Staffing Firms

This alert addresses a recent 6th Circuit Court of Appeals decision, *Perry v. Randstad Gen. Partner (US) LLC*, 2017 WL 5560160 (6th Cir. Nov. 20, 2017) (See link to decision below), concerning classification of employees as exempt versus nonexempt. "Exemption" classification, much like independent contractor classification, is highly fact intensive, nuanced and specific. And, as with independent contractor classification where workers are presumed to be employees unless proven otherwise, employees are presumed to be nonexempt unless proven otherwise by the employer. So, exemption misclassification is another of the many areas of employment law providing legal risk and uncertainty to employers.

Amidst an environment of legal uncertainty, staffing firms seeking to classify their account managers as exempt now have some instructive case law. Specifically, the *Perry v. Randstad* decision held that certain account managers working for temporary staffing firm, Randstad, performing the "primary duties" of matching and placing workers with clients and overseeing placements (which the court called "exempt matchmaking

front-of-mind right now, those that most people are most anxious of or interested in, deal with the politics of our time and the manner in which we are addressing the societal and national issues confronting us. Being a generally polite person, I also believe that there are few more dangerous things in any social circle than to share your unvarnished opinion about the politics and issues we currently face without knowing your crowd. At most parties, conferences, meetings – or opinion pieces in newsletters (!) – there is, it seems, a risk in lobbing an opinion about gun control, immigration, or some other flavor of the day into a crowd whose sensitivities you have not previously known. And the risk seems far worse now than in prior years as differences of opinion widen.

As a result I typically start

duties") exercised discretion and independent judgment sufficient to meet the FLSA's administrative exemption. However, the court also held that another category of employees at the company, called staffing consultants, were nonexempt because their "primary duties"- - described as "sales and routine recruiting tasks"- -lacked sufficient discretion and independent judgment.

This case is not binding on California state or federal courts as the 6th Circuit has jurisdiction over Michigan, Ohio, Kentucky and Tennessee. And, California has its own exemption test that differs from federal law. Nevertheless, this decision may be useful as persuasive authority in other courts. Here is the link to the *Randstad* decision: https://www.leagle.com/decision/infco20171120106.

Please contact Denis Kenny at (dsk@sfcounsel.com), Ryan Stahl at (rws@sfcounsel.com), or John Lough, Jr. at (jbl@sfcounsel.com) for more information on upcoming laws that may affect your workforce, scheduling a mandatory harassment training, or assessing and updating your workplace policies to ensure compliance with controlling law.

-Written by Denis Kenny

New California Employment Laws for 2018

2018 is now fully upon us. And with the beginning of a new year, one certainty is that there will be new employment laws to become familiar with in California. Below is an overview of three new laws related to salary history inquiries, criminal history inquiries, and parental leave that employers should understand and begin implementing this month.

SB 63 – Expanded Parental Leave

Before 2018, the Family Medical Leave Act ("FMLA") and the California Family Rights Act ("CFRA") required employers with fifty or more employees to provide up to twelve weeks of unpaid leave leave for a number of reasons, including the employee's own serious health condition; the employee's need to care for certain family members with a serious health condition; and the employee's need to bond with a new child.

Senate Bill 63 – entitled the New Parent Leave Act – now extends the right to up to twelve weeks of unpaid leave to employees of smaller employers – those with at least twenty employees – for the employee to bond with a new child. The same tenure-of-employment criteria still apply to such leave as currently exist under FMLA and CFRA. Namely, any employee wishing to take such protected leave must have worked at least 1,250 hours for the employer in the twelve-month period preceding the beginning of the leave period.

Under the New Parent Leave Act, the employer must also continue to pay for any coverage for the employee under a group health plan on the same terms and conditions as were offered to the employee before the leave began. Additionally, while the employer must allow the employee to use any accrued vacation leave, sick leave, or paid time off, such leave is otherwise unpaid. The New Parent Leave Act does not provide additional

conversation in any gathering by probing my audience's politics and point of view. "Where do you live," or "Where are you from," or "How do you like working in/visiting [name of city]," etc. provides some insight into political and social sensitivities and informs what kind of conversation might be held. Even in San Francisco, viewed nationally as homogenously liberal, even radical, you wade into social and political issues at your own risk.

What causes this divide? Perhaps it's the echo chambers of social media that reinforce opinion by sharing only the posts of like-minded members, the bitter Congressional divide, the anxiety that issues that affect us all are not being addressed, or some other reason. But speaking your mind has never been more perilous.

protected leave rights to employees of employers with between twenty and forty-nine employees for the employee's own serious health condition or to care for family members with serious health conditions.

AB 1008 – "Ban the Box" Expanded Statewide

In 2013, California passed legislation prohibiting state agencies and subdivisions (such as cities and counties) from asking job applicants about past criminal convictions. In 2015 under a directive from President Obama, federal agencies adopted the same prohibition. These have colloquially come to be known as "ban the box" laws as they prohibit asking a job applicant if he or she has any prior convictions, which typically occurs by asking the applicant to check a box "yes" or "no."

Under Assembly Bill 1008, the prohibitions related to conviction history inquiries will now apply to all California employers with five or more employees. As of January 1, 2018, Employers are prohibited from making any inquiries into conviction histories until at least a provisional offer of employment has been extended to the prospective employee.

At the point such an offer has been made, conviction history inquiries become possible but with several caveats:

First, several types of incidents that may show up on a background check may not be considered by the employer. These include arrests not followed by a conviction, referrals to participation in a pretrial diversion program, and convictions that have been sealed, dismissed, expunged, or statutorily eradicated pursuant to law.

Second, if the employer intends to deny any applicant a position based on a conviction, this may only be done following an assessment that considers a number of individual factors. These factors include the nature and gravity of the offense, the time that has lapsed since the conviction, and the nature of the job.

Third, if the employer makes a decision that the conviction is disqualifying, the applicant must be notified of the decision in writing. This notice must include a copy of the conviction history report that was relied upon, if any, and explain to the applicant that he or she may respond to the notice before the decision becomes final. If the applicant submits an explanation in response to the notice, the employer must then consider this explanation. If the employer still decides the conviction is disqualifying, then the employer must again notify the applicant in writing of its decision. This notification must further explain to the applicant that he or she has the right to file a complaint with the California Department of Fair Employment and Housing regarding the employer's decision.

AB 168 – Salary History Information

Also newly effective as of January 1, 2018, is Assembly Bill 168, which places restrictions on information an employer may seek from an applicant for employment related to past salary history. Under this new law, an employer may not ask about or rely on salary history information in determining whether to offer a job to an applicant or what salary to pay that applicant. This new law also obligates an employer to provide a pay scale for the position applied for upon the applicant's request. There is an exception to this prohibition, however – if the applicant voluntarily discloses past salary history to the prospective employer, the employer may then consider this salary history in setting the employee's salary.

So that, readers, was the issue. God knows I have plenty of opinions. I just didn't feel I could share them within a light, conversational article without offending some in the audience. If I know you personally I will certainly share, but for this piece, sent out to hundreds of our clients, it seemed like a risk not worth taking. But then again, perhaps this conundrum gave me a pretty good alternative topic to write about.

So for the record and in connection with any conversation we might have in the future, please know that I will always respect a point of view and the communicator of that opinion. Hopefully, I can hope for the same. However, I do not promise I will agree with any particular point of view, and I don't require anyone to agree with me. Following these general guidelines have given me many

As detailed above, the landscape of employment laws in California is constantly expanding, and in many cases these new laws create new and nuanced administrative responsibilities for employers. While sometimes seeming onerous, failing to understand and properly adhere to the requirements of these new laws can result in employer liability. We here at Scherer Smith & Kenny LLP remain available to address any questions you may have related to these new laws and any other employment- or business-related issues. For additional information, please contact Denis Kenny at (dsk@sfcounsel.com), Ryan Stahl at (rws@sfcounsel.com), or John Lough, Jr. at (jbl@sfcounsel.com).

- *Written by Ryan Stahl*

very enjoyable, very enlightening discussions.

Written by William Scherer

Areas of Practice

Business; Real Estate; Intellectual Property and Employment Law; Litigation and Dispute Resolution; Nonprofit; Estates and Trusts