June 2015

Contra Costa Lawyer Online

The Contra Costa Lawyer is the official publication of the Contra Costa County Bar Association (CCCBA), published 12 times a year - in six print and 12 online issues.

Contents

Inside: Guest Editor's Column, June 2015

Monday, June 01, 2015

"Historically, privacy was almost implicit, because it was hard to find and gather information. But in the digital world, whether it's digital cameras or satellites or just what you click on, we need to have more explicit rules—not just for governments but for private companies."
- Bill Gates

What is "privacy"? Does it even exist anymore? Do we care or will we read this, think of something witty (and short) to say in response, and tweet our answer to all of our followers?

In today's day and age, the concept of privacy is a quickly changing one. As Bill Gates points out, it used to be an implicit idea—people knew only what we chose to share about ourselves because it was very hard (and very unlikely) that they could gather that information otherwise.

Not anymore. Our phones have GPS trackers. We tweet and post our every thought on Twitter or Facebook. We take photos of what we ate for breakfast (as if *anyone* cares what we ate for breakfast). We have voluntarily put so much information out there, that the question of whether "privacy" even exists at all is a legitimate one.

Technology is pushing this conversation even further. There are drones that can fly above us and look down upon us, recording our every move. Many cities have so many traffic cameras placed about that our every move can be tracked. Search engines have become so good that it is not very hard to find out whatever you want to know about pretty much anyone.

In this quickly changing landscape, it is important to stop and ask, "What is privacy and does it exist anymore?" In this issue of the *Contra Costa Lawyer*, we will look at this question from different viewpoints, examining what privacy means and how to best protect what privacy we have left.

James Wu has written a wonderful article about privacy at work. In that article, there is a link to a speech given by Former Chief Judge Kozinski, called "The Dead Past," and I really encourage everyone to read it. It is one of the best examinations of privacy and our dwindling "right to privacy" that I have seen. Privacy as a concept is quickly disappearing and if we are not careful, it will soon be too late to save it. As Judge Kozinski concludes, "If we the people don't consider our own privacy terribly valuable, we cannot count on government—with its many legitimate worries about law-breaking and security—to guard it for us."

It might also be interesting to consider the prescient words of James Madison, written around 200 years ago:

“Wherever the real power in a Government lies, there is the danger of oppression. In our Governments, the real power lies in the majority of the Community, and the invasion of private rights is chiefly to be apprehended, not from the acts of Government contrary to the sense of its constituents, but from acts in which the Government is the mere instrument of the major number of the constituents.” - *James Madison*, “Letters and Other Writings of James Madison Volume 3”

We will lose our “right to privacy” not because someone has wrested it from us, but because we have given it away … we have tweeted it away … we have posted it away.

- *Jane Doe*

Privacy, Innovation and the Internet of Things

Monday, June 01, 2015

In his recent address to Japan, Charles Rivkin, Assistant Secretary of State for Economic and Business Affairs, analogized the Internet with a story from Aesop's Fables, specifically that of "The Goose that Laid the Golden Eggs." In the story, a feathered animal produced gold and acted as the source of profitability for its owners. In their shortsighted actions however, its owners killed the goose.

Rivkin stated that the Internet is a modern equivalent of a gold-producing goose. With its connections come data and economic activity that make it an indispensable tool in almost every human endeavor. Still, the Internet has much untapped potential and over three billion people are connected to it.

For legal professionals, things are becoming more digital by the day. A whole industry has emerged based on e-discovery; firms are becoming virtual with the use of Internet based-legal services such as LegalZoom or Lex Machina, and even with the advent of remote lawyering (through such services as Beam Smart Presence).

Further, with social media, networking is often an entirely digital affair. To this end, LinkedIn is a place where legal professionals share their resume and a platform for clients to research attorney profiles; Twitter is a place for attorneys to post 140-character messages to be shared with the world; and let us not forget the array of possibilities for attorneys on Facebook.

With all of the information stored digitally on the Internet or in the cloud, *how do we address the emerging problem of privacy protection and data security*?

Samuel D. Warren and Louis D. Brandeis authored a famous article on "The Right to Privacy," published in the Harvard Law Review in 1890. The article pinpointed that "the principle which protects personal writings and any other productions of the intellect of or the emotions is the right to privacy." Since then, privacy has been a valuable concept, especially with the increase in technology. In the United States, there are specific laws in place to protect privacy in the financial or health industries. There are also general consumer protection laws against unfair or deceptive practices.

With the new developments in technology such as: wearable health gadgets; Internet-connected cameras that allow you to post photos onto the Internet with a single click; automated systems that allow you to control your home porch lights remotely and more. The Internet of Things (IoT) is among us and presents various risks to consumers regarding data security and privacy. Such devices offer numerous and even revolutionary benefits to consumers, especially health devices, which can improve the quality of life for many. Still, they come with enormous risks.

The IoT explains the interconnected system of communicating with objects and people through the digital sphere. These systems store, transmit and share a vast amount of

consumer data, some of which is highly personal. Already the Federal Trade Commission (FTC) has expressed its concern with the IoT and has sought to explore various smart devices. These devices produce privacy risks to businesses regarding: breaches and civil suits, loss of consumer trust, a devalued brand and more.

According to the FTC report on the IoT, smart devices may exploit or harm consumers by enabling unauthorized access to personal data, facilitating attacks on other systems or even creating safety risks. Smart televisions, for example, may store personal financial data, passwords, addresses and other sensitive information. A compromised or hacked IoT device may make the user susceptible to various service attacks as well, such as harmful emails. Further, hackers may even present safety risks to users by changing the settings on their designated devices.

An example of this is with health devices that store diabetes-related insulin with pump delivery to users. Another example is with regard to changing the settings of one's vehicles. Here, risks can be amplified with the increase of automated cars and other automated objects. Similarly, fitness device tracking may pose a physical safety threat to others or may even allow a thief to know when a person is not at home.

Moreover, because many of these issues are novel, companies in the IoT market may not know how to properly protect data, and may not know how to address security issues. The utter amount of data that devices may hold is stunning. The FTC provided an example of this with regard to home-automation products in stating that such devices may generate "150 million discrete data points a day."

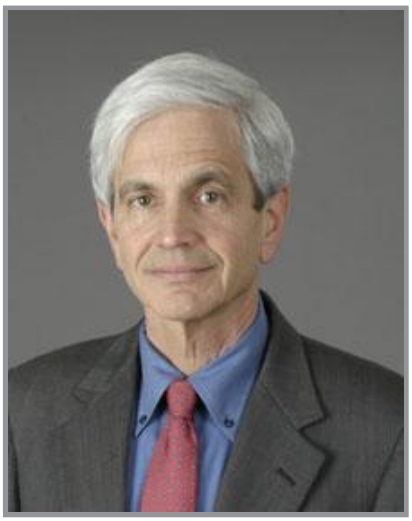
Smart IoT device sensors may track mood, health, personality-type, stress level and more. This collection of behavioral patterns may prove difficult if in the wrong hands. The data collected may be used for pricing gadgets, for personalizing other products and even more consumer uses. Another risk may be that manufacturers of such devices may eavesdrop remotely on users by analyzing unencrypted data transmitted through the device.

Furthermore, smart IoT gadgets are the way of the future, but must be approached with caution. We share the conviction that the Internet must remain an open and lively platform that promotes such innovation. However, we must be mindful of the information we are putting out through such smart devices and how the information is stored and used. After all, we would like to preserve our golden egg-bearing goose for as long as possible.

***Angela Habibi**, J.D., is an intellectual property LL.M. candidate at Santa Clara University School of Law and an IAPP data privacy and security professional.*

Privacy vs. Public Access in Civil Cases

Monday, June 01, 2015



Pursuant to Rule of Court 2.550(c) and its predecessor, California court records have long been "presumed to be open" to the public, absent exceptions for confidentiality required by law.

Just 10 or 15 years ago, accessing civil court records in California and elsewhere was an arduous task: It took a great deal of effort to get information from court files. An "inquiring mind" had to go to the county clerk's office, borrow the desired physical court file, go to an adjacent public access area, and copy the desired file portions on the court's copy machine. The court's file could not leave the premises.

Contrast those past procedures with public access to court files today: Most courts have an accessible online database. In many counties, often for a fee, one can obtain and save to a computer (or print) virtually any civil filing by any party in any civil case. Sites like DomainWeb in Alameda County allow the user to enter a case number, go through an index of all court filings in that matter from beginning to end, then select any desired documents for access and copying, for a fee.

Contra Costa County permits online access, without charge, to all documents filed in complex litigation cases, but not non-complex cases. San Francisco County makes some filings in civil cases viewable without charge, and others accessible for a fee; but it leaves some filings unavailable for online viewing. No basis for this differentiation is readily apparent.

San Mateo County allows many filings in civil cases to be viewable online in PDF format, without charge. Marin and Solano counties permit the Register of Actions to be viewable online, but individual filings are not. While Bay Area counties differ significantly in how they permit online access, the trend is towards permitting greater public access to civil case filings; and, of course, one has ready access to civil file content at the clerk's office.

These technological advances providing online access to the public constitute a real revolution, but there is a dark side: the loss of litigant privacy. Open access to court records can represent more than just the public's opportunity to view lawyers' mundane presentations about a civil case; they can be an invitation to the invasion of litigants' privacy.

Take, for example, the following hypothetical: Jane Doe, age 25, has an ongoing personal injury case wherein one issue is the nature and extent of physical and psychiatric damages that she sustained resulting from sexual abuse by a clergyman.

The public record in the case might include Settlement Conference Statements, or other documents filed by the parties, which contain (among other personal information), details of the alleged sexual acts underlying the claim as well as the plaintiff's asserted injuries allegedly resulting from them. Attached to such statements could be medical records and

physician reports disclosing Jane's otherwise confidential physical and psychiatric conditions, both incident-related and otherwise.

Consider the instant availability of this sort of information in light of the growing popularity, over the past decade, for employers, landlords and others to use fee-based search services to comb the Internet to get the litigation history of prospective employees or tenants, to ascertain whether that history might affect (in the purchaser's view) his or her suitability for employment or tenancy.

Such a search might theoretically produce a psychiatric report disclosing Jane Doe's bi-polar diagnosis, her sexual history and her current medications. While technology did not make this private information appear in public court files (it may have been there all along), it has made confidential personal information infinitely more *accessible* to those seeking it.

There are a few approaches to addressing this dilemma of which counsel for parties whose confidential information is at issue should be aware. The first key is simple: be aware of the issue. That awareness might lead counsel to limit disclosure of a client's personal information in filed court documents in the first place, particularly in filings (like pleadings) where providing such intimate detail may offer no real benefit in the first place.

In Jane Doe's case, counsel cognizant of this issue might have stipulated with opposing counsel that reference to her physical and mental condition, and confidential records related thereto, would be presented to the judge *in camera* during the settlement conference only, not made part of a public filing.

Another potential solution would be moving to seal documents pre-filing. CRC 2.550(d) addresses when a document may be filed under seal. Drafted primarily to protect public access to the courts, it states:

"The court may order that a record be filed under seal only if it expressly finds facts that establish:

(1) There exists an overriding interest that overcomes the right of public access to the record; (2) The overriding interest supports sealing the record; (3) A substantial probability exists that the overriding interest will be prejudiced if the record is not sealed; (4) The proposed sealing is narrowly tailored; and (5) No less restrictive means exist to achieve the overriding interest."

An order obtained by a party sealing a record must specifically state the facts that support these findings.[1] The court must not permit a record to be filed under seal based solely on the agreement or stipulation of the parties.[2] The procedure for filing a motion or application to seal a record is set forth in Rule of Court 2.551(b).

Utilizing these Rules to seal confidential documents at the time of filing, like Jane Doe's Settlement Conference Statements, is a potential solution to protecting her privacy. If the statements are sealed when filed, the court can still review them, and confidential medical reports and records attached to them, to evaluate the underlying case; but there is no *public access* to the plaintiff's confidential information.

Finally, case law offers a solution when there is no pre-filing order to seal, and a litigation opponent files documents revealing the other party's confidential personal information

(for example, if Jane Doe is concerned because the defendant publicly filed her confidential medical records as an exhibit to his Settlement Conference Statement, and/or discussed them in his statement).

In *Oiye v. Fox* (2012) 211 Cal.App.4th 1036, 1068, *review denied (Mar. 13, 2013)*, the defendant in a civil sexual abuse tort case included, in an injunction opposition, medical reports and diary excerpts relating to and discussing the plaintiff's personal psychiatric condition and medical history. On the plaintiff's motion, the trial court granted (and the appellate court upheld) an order *sealing* those exhibits post-filing, irrespective of the limitations otherwise applicable under CRC 2.550 *et al.*

Citing to the plaintiff's rights under the Confidentiality of Medical Information Act[3], the court at 1068 rejected the defendant's contention that the requested relief should be denied because the plaintiff's psychiatric condition was properly at issue in the case: "However, disclosure to an opponent in civil litigation does not necessarily waive the patient's privilege to keep the information from third parties, including the public."

In summary, counsel should take all reasonable steps to protect a client's confidential personal information. Those steps should include: (1) minimizing disclosure of such information in court filings, in the first place; (2) stipulating to, and then obtaining a court order permitting, pre-filing sealing of all documents filed by any party that include any party's confidential information; and (3) moving to have sealed (or, post-litigation, deleted) filings by litigation opponents that contain confidential personal information of a party.

Public access to court records is not an absolute good; it should be favored only to the extent that the privacy interests of litigants are offered appropriate protection. Counsel should take steps necessary to protect clients' privacy rights in that regard.

Ralph L. Jacobson *is a founding partner of, and now of counsel to, the law firm of Gillin, Jacobson, Ellis, Larsen & Lucey in Orinda.*

[1] CRC 2.550(e).

[2] CRC 2.551(a).

[3] Civ Code § 56 *et seq*.

No Privacy at Work? Is Social Media to Blame?

Monday, June 01, 2015

"What is my right to privacy at work?" Employees ask this question a lot, and mostly assume that they have an unlimited right to privacy. Conversely, employers generally maintain that their employees have a limited right to privacy. These conflicting viewpoints arise in various employment contexts nearly every day.

We analyze them when an employee is being questioned about his or her Internet use at work, and when an employee gets caught posting about how much fun it is being at a baseball game on a day he or she called in sick. We debate them when an employee sends a sexy text using a work-provided smartphone. And, we litigate these issues during employment litigation when employees want to prevent an employer from using as evidence their very own texts, posts, pictures and status updates.

What is the correct answer to such a ubiquitous question as "What is my right to privacy at work?" As lawyers like to say, "It depends." This is so because the number of specific laws on workplace monitoring/privacy is small. And, thus, "it depends" arises quite frequently.

What is a Reasonable Expectation of Privacy?

In these situations, an employee's right to privacy is governed by an amorphous standard that focuses on an employee's "reasonable expectation of privacy" in the workplace. Former Chief Judge Alex Kozinski of the U.S. Court of Appeals for the 9th Circuit, spoke about this topic at a Stanford Law Review Symposium, and his presentation, titled "The Dead Past," was published by the Stanford Law Review Online. Judge Kozinski dissected the notion of what is a "reasonable expectation of privacy" and how it is changing rapidly due to technology and everyone's use of it.

While his article did not focus specifically on social media and employment law, it does raise some very thought provoking questions about our society's expectations of privacy, and those expectations help define what is, or is not, considered private in the workplace. Judge Kozinski essentially advances the notion that we (everyday people), and not the government, nor "Big Brother," are eroding the expectation of privacy.

For example, we have sensitive (private) conversations on cellphones in restaurants, walking down the street and at airport lounges. We check in, update our status and post silly videos without much thought to the permanency and widespread distribution of such content (even if your privacy settings are on).

As Judge Kozinski notes, we post details of sexual affairs and go on national television to talk about them openly. Technology is leading us away from private one-on-one discussions. Instead, technology is helping all of us broadcast too much information. And, a potential consequence of such TMI is the erosion of the expectation of privacy.

What Employers Do, and How Do They Do it Lawfully?

Employers have a legitimate interest in making sure their employees are working during work time, being productive and using company-provided computers/equipment for legitimate business purposes. Today, some employers block all access to non-work related websites. So if job tasks do not require activity on Facebook, Twitter, Google+ or LinkedIn, some employers block access to such sites along with many others. Some employers also deny workplace computer access to email run through third-parties, like Gmail, Yahoo! and Hotmail.

A greater number of employers, however, do not block such sites and email services, but rather maintain the option to monitor employee computer, Internet and telephone use. They do so lawfully because they tell their employees that they should have no expectation of privacy. Generally, employers have a great deal of latitude monitoring their employees, if done for legitimate reasons, and done in as limited a way to achieve these legitimate reasons.

Employers should have policies that make clear in no uncertain terms that when an employee uses company-provided computers, Internet access or other property, the employee consents to being monitored. These policies are generally found to be lawful, particularly when the employer owns the computers/equipment and/or the email system/Internet access. Furthermore, employees usually acknowledge their understanding of such policies by signing an acknowledgement form about the specific policy, or about an entire employee handbook that includes such provisions.

With such knowledge, employees have difficult, and usually unsuccessful, arguments that their use of their employer's computer system for personal reasons during work is protected by their right to privacy. Simply, they should have had no expectation of privacy because the employer's policy explicitly said as much. Whether an employer actually monitors all such activity is another question, and there are limits on all of that.

The important takeaway here, however, is that if an employer promulgates properly drafted policies and notices, employees should not consider anything done using company-provided tools to be private.

The case law around the country continues to develop on issues of employer monitoring and employee privacy. For example, the U.S. Supreme Court, in June 2010, unanimously held that a search of a police officer's personal messages on a government-owed pager did not violate his constitutional right to privacy.[1] The Supreme Court determined that the search was motivated by legitimate business reasons, and thus, the employer did not violate the employee's right to privacy when it discovered the sexually explicit text messages he had been exchanging.

Other cases have examined the issues of whether an employee has differing expectations of privacy while using his or her company's computers to send emails from a work email account versus using the company's computers to send emails from a third-party email provider (like Gmail).

Additionally, in California, on September 27, 2012, Governor Jerry Brown used Twitter and Facebook to announce two new laws (AB 1844) that he had signed regarding social media. He wrote: "California pioneered the social media revolution. These laws protect Californians from unwarranted invasions of their social media accounts."

Generally, California employers now face specific restrictions regarding access to their employees' social media accounts. And, California employers are now prohibited from discharging, disciplining, threatening or otherwise retaliating against an employee or job applicant for not complying with the employer's demand for social media access.

Generally, even before these new laws, employers should not have been asking applicants and/or employees for social media login credentials or information, as doing such could be considered a breach of the social media site's user agreement, and could give rise to unintended lawsuits regarding discrimination and retaliation, for example. As a result, the California law is a bit of overkill to address an ill-advised practice that most employers do not, and never did, engage in.

An employee's right to privacy while at work is limited. Employees should take care in how they use employer-provided equipment and systems, and frankly, wait until they get home to post something on Facebook, or to tweet (unless they do not care if their employer has access to their online activities).

And employers should be cautious too. While employee monitoring is generally permissible, it does not mean employers should routinely do it, nor does it mean, as the National Labor Relations Board advises, employers can always take action on something posted by an employee at work.

The original version of this article, titled "Social Media Privacy in the Workplace: Is There Any?" first appeared online on July 3, 2012, at http://maximizesocialbusiness.com**.**

For nearly two decades, ***James Y. Wu*** *has provided employment law advice and counsel, and litigation representation, to employers of all sizes. James is a member of the Executive Committee of the CCCBA Board of Directors, and former President of the CCCBA Employment Law Section. Learn more at* www.wucastillo.com *and* http://www.linkedin.com/in/jamesywu*/.*

[1] *City of Ontario v. Quon*

Privacy Protections in the Juvenile Court

Monday, June 01, 2015

As a general rule, all Juvenile Court proceedings are closed to the public. There are two types of juvenile proceedings: juvenile delinquency and juvenile dependency. Delinquency proceedings relate to children who commit acts which would be considered crimes if committed by adults; while dependency proceedings relate to children who are at risk of abuse or neglect because of an act committed by a parent.

In both cases, a petition is filed under the child's name. These hearings are private because both of these proceedings are ultimately designed for the protection of the rights of the children, as opposed to the rights of the general public.

In delinquency proceedings, the child is present in court and must answer the allegations that have been filed by the District Attorney's Office. The child has an attorney to defend the allegations. The child's immediate family is allowed inside the courtroom. There is no jury in juvenile cases; the judge makes all the decisions.

The public does have some right to know what is going on. For example, the victim of the acts of the child who is before the court has a right to attend the hearings; the victim can give a statement to the court and can often ask for restitution. The court can also grant stay-away and restraining orders to protect the victim. The crime victim can attend the hearings and may often bring a support person.

But, because these are children, who we hope will not continue to be involved in criminal activity, they are protected from the scrutiny of open court proceedings they might be subject to if they had committed the same act as an adult.

There are some exceptions to that general rule. If the crime is so serious that the child is tried as an adult, then the child loses the privacy protections of the juvenile court. If the child is certified for treatment in adult court, then the general public and the press will have the same access to information as they would for an adult.

In juvenile dependency proceedings, the child is the victim. The child is before the court

because of abuse or neglect at the hands of their parent(s). These cases often involve very sensitive information. Most involve some sort of substance abuse by the parent. Many others are brought to court due to violence in the home, domestic violence and/or physical violence against the child. There are also cases where children have been victims of sexual abuse.

These children are not before the court due to anything they have done. They have often been removed from their parent(s) and placed in foster care. Many have had to change schools, be separated from relatives or siblings and all of their familiar surroundings. These children need the protection of the court to keep their information private so that they can heal from their ordeal.

Just as in delinquency hearings, there is no jury for juvenile dependency court; the judge makes all the decisions. County Counsel represents the Department of Social Services, the child has an attorney and the parents are also entitled to attorneys to represent their interests. Sometimes other family members want to attend these hearings. Their presence inside the courtroom is at the discretion of the judge and they may be allowed inside if no party objects.

There is a mechanism to gain access to information about these private hearings outside of the criteria mentioned. Under Welfare and Institutions Code Section 827, a person may file a petition with the court to gain access to court records of the child for certain limited purposes. A judge reviews the file and determines what information may be disclosed. Even this disclosed information is subject to certain limitations and may only be used for certain purposes—perhaps in some other court proceedings where it is deemed necessary.

Despite all of these protections, one appellate court has noted that allowing media access in juvenile proceedings promotes the fairness of the proceeding, improves juvenile court practice and serves to check abuse of judicial and governmental regulation that may interfere with the constitutional right of parents to decide how to raise their children.[1] Any right that the general public may have to access confidential juvenile proceedings and records must take into account the need to protect the privacy rights of the child.

Rhonda Wilson-Rice *is an attorney in Contra Costa County. Her practices area is Juvenile Dependency, Juvenile Delinquency and Criminal Defense. She is the chair of the Juvenile Law Section of the Contra Costa County Bar Association.*

[1] *See San Bernardino County Dep't of Public Soc. Servs. v. Superior Court* (1991) 232 Cal.App 3d 188, 201-203.

Drones in the Contra Costa Skies

Monday, June 01, 2015

Drones, drones, drones. They are all over the news recently. Whether it is their use by the government to kill enemies of the state or proposals by Amazon to have orders delivered directly to your home, drones are all the rage. So, what is a drone? Merriam-Webster defines a drone as “an unmanned aircraft or ship guided by remote control or onboard computers.” However, others take a more restrictive view of what vehicles fall into the “drone” category.

Since there have yet to be any military drone strikes in the U.S., this article will focus on non-military drone uses and then only superficially, as lawyers and others are still trying to grapple with the quickly advancing technology. The three areas of drone use most concerning to the average person are police use, commercial use and personal use. All three of these uses are interrelated and laws being passed or debated will have multiple, far reaching effects which will not be fully known or understood for years.

There are many thorny issues related to privacy, particularly when drones are being developed that can fly continuously for five years. Consider the case of *California v. Ciraolo* (1986) 476 US 207, where the Supreme Court held that the Fourth Amendment does not require police traveling in the public airways to obtain a warrant in order to observe what is visible to the naked eye.

Now imagine a drone hovering over your neighborhood, at a height of 50,000+ feet for years at a time, watching and recording everything that occurs outside. Talk about the ultimate red light/speeding camera.

Police Use

In California last year, Governor Brown vetoed Assembly Bill 1327 to require police to obtain a warrant before their use of drones. The only exceptions when a warrant wasn't required were "emergency situations," such as fires, hostage crises, chases, search and rescue and environmental disasters. The Governor indicated in his veto message that the bill's exceptions to the warrant requirement were too narrow and might impose requirements beyond the Fourth Amendment or the California Constitution.

In response to this attempt to limit the use of drones by police, the California Police Chiefs Association has sponsored a bill, SB 262, which would authorize police to use drones as long as they comply with "protections against unreasonable searches" in the United States Constitution and the California Constitution and any other applicable state or federal law. The American Civil Liberties Union (ACLU) is fighting SB 262 as a significant infringement on privacy rights, and AB 1327 has been reintroduced as AB 56.

For now, this is somewhat of an academic argument. So far, drone use by police departments has been extremely limited, if used at all, due to regulatory restrictions. In order for a department to deploy drones, they first must go through a Federal Aviation Administration (FAA) application process that is lengthy and complex.

The FAA recently released a set of proposed rules and is in the process of gathering comments. The new rules would allow commercial and law enforcement use of drones under 55 pounds so long as the operator passes a written test, registers the drone and pays a fee. Because the rules are still in the comment stage, it will be years before a final version is adopted, which will slow police use.

Commercial Use

The FAA recently granted Amazon, the 1,000 lb. gorilla in the retail space, an exemption so that it can begin testing the use of drones to deliver Prime Air service. To conduct research for a proposed drone-delivery program, Amazon will be able to fly up to 400 feet high at up to 100 miles an hour over private property and within sight of the remote-control pilot or a designated observer. The flights are supposed to remain at least 500 feet away from other people. If the aircraft loses the connection to its pilot or GPS signal, it must return to a predetermined location.

Many other commercial exemptions have recently been granted by the FAA for activities such as movie making, agricultural monitoring and aerial surveys. Commercial use, other than by photographers, is also still in its infancy due to FAA rules.

At the state level, SB 142, introduced this year, would make it a crime to fly a drone over private property without permission. This is on top of AB 2306, signed into law on September 30, 2014. AB 2306 amended Civil Code 1708.8 to impose severe civil penalties on individuals using drones to take pictures of people when they had a reasonable expectation of privacy. This amendment was specifically aimed at paparazzi and includes hefty damages and fines.

Personal Use

With the introduction of cheap, personal use drones, many people are concerned with their creepy neighbor or the neighborhood teens flying a drone over their backyard and video recording everything. Personal use drones with video capability can be purchased for as little as $199. This gets you a drone with limited flying distance and without any real-time camera viewing. This means that all photos or videos have to be stored on a card and viewed later, which greatly reduces accuracy.

For one with a real-time camera that will stream to your iOS or Android device, one needs to spend closer to $700. These types of drones still shouldn't cause much of an issue at this point. They are limited in how far from the pilot they can fly, so tracking down the owner isn't difficult. With time though, inexpensive drones will continue to improve their distance from the owner, camera quality and, ultimately, the ability to use pre-programmed routes using a GPS, much like commercial and government drones.

That said, it is a personal use drone that is behind SB 142, discussed above. Sen. Jackson (D-Santa Barbara), wrote the bill after a neighbor's camera equipped drone flew into her backyard and took pictures of her and her husband and guests.

Lawmakers are only starting to grapple with this nascent technology. If their efforts in other technology areas are any example, there will be significant overreach without much understanding, while the technology continues to outpace the law.

David Pearson *is a solo practitioner who works from his home in Walnut Creek. Since striking out on his own in 1996, he has concentrated his practice in the representation of closely held businesses and their owners with both transactional and litigation matters. David can be reached at attorney@mac.com.*

How to Protect Your Passwords

Monday, June 01, 2015

Passwords. So. Many. Passwords. How can I remember so many passwords? At the end of the day, this is how many of us feel, and it is one reason that 66 percent of people online use only one or two passwords for all of their accounts. We *know* that isn't a good idea, but we do it anyway, and it may be our undoing.

One of the No. 1 tips for password protection and safety is not to use the same password for more than one account, but how do we do that and still remember all of them?

Here is a list of tips for remembering and securing your passwords:

- Use a passphrase instead of a password. It can be a sentence or a random string of words (even better) or it can be the first letter of the words in a sentence. All of these are stronger than a password, which is much more easily hacked.
- Turn to technology. Utilize a password generator or a password strength tool to help you create stronger passwords. Use a password manager to help you access numerous passwords via one, stronger password.
- Change your passwords often. Using old passwords increases the chance of being hacked.
- Do not share your password with anyone. It should go without saying that you should not share your passwords with most people. Whether you share them with your spouse or partner is a question each person should address for themselves, but one source found that only 32 percent of Americans surveyed reported that they knew their spouse's online or banking passwords, suggesting that two-thirds of us are not sharing our passwords even with our significant others.

To be fair, the number may be higher, as the study did not ask people *how* they knew their spouse's passwords, just whether they knew or not.

On the other hand, "The survey also discovered, however, that other passwords are shared more readily. More than half (55 percent) of those surveyed in the United States, for instance, know their partner's Facebook password (and vice versa). Just under half (46 percent) indicated they know their significant other's email or PC password, and 45 percent reported knowing the other's cell phone password."[1]

We have all heard these tips more times than we would like to admit, and yet many of us (often to our detriment) disregard them anyway. If you would like to read more about password protection, here are some links you might find helpful:

- "Secure your passwords," Google Safety Center
- "Password security tips: When and how to share them safely with loved ones," PCWorld
- "Passwords: Fascinating Facts and Smart Tips for Mankind," HalockSecurityLabs
- "Create secure passwords to keep your identity safe," Mozilla Support
- "Online Security," Blackhawk Bank; *see* "How Passwords Are Stolen" section at the very bottom.

[1] "Password security tips: When and how to share them safely with loved ones," PCWorld

Inns of Court: Revenge Porn and the Law

Monday, June 01, 2015

On April 9, 2015, Judge Cheryl Mills' pupilage group (starring David Pearson, Bonnie Johnson, Susan Aglietti, Jon Wolfe, Jill Lifter, Joseph Ryan, David Marchiano and Jeremy Seymour) discussed technical advancements in shaming others (i.e., revenge porn).

Revenge porn is where people upload naked photos of others to the Internet without their consent. This is a new and complex crime that was not well known in the world until recently. In fact, revenge porn was not illegal in a specific statute until 2013.

The presentation started with two vignettes that touched on these technological issues. In the first vignette, Susan and Bonnie dished about their fictional grandchildren. Susan's character's granddaughter was dating the 17-year-old football star at high school. Here, the football player inappropriately sent videos of his girlfriend to his friends.

In the second vignette, David Marchiano and Jon Wolfe discussed a boyfriend who threatened to distribute naked photos of his girlfriend without her consent, which is an extremely no-chill thing for that bro to do. These crimes are not extortion, because no money is involved. However, they are potentially revenge porn, for which there is both a criminal and civil cause of action. In general, it is defined as the intentional distribution of pictures or videos with the intent to cause distress and the distribution actually causes distress.

David Pearson then discussed various social media sites. There were the basics, such as Facebook and Twitter, lesser known ones like Tumblr, extremely new ones, like Yik Yak, and ones that he created for this very presentation. Nobody there was cool enough with "the kids" to know he was making them up! How could we have known that www.DavidPearson.com is not a super popular site with the kids these days?

In all, it was a terrifying review of the ways that our children are lying to us. My daughter is only 18 months old and she is already more technically advanced than every boomer ever. So no matter how vigilant we are in stalking our kids across any number of social media sites and apps, these younger generations will always be many, many steps ahead of us. I think I speak for parents everywhere when I say that wherever we go, we instantly make that site extremely lame. We singlehandedly drive our kids away from these sites like Moses seeking the land of milk and honey (currently, Instagram).

Jeremy Seymour then discussed a recent court case involving revenge porn. The key person here was Kevin Bollaert, who ran YouGotPosted.com. At that website, people could anonymously upload naked photos of others without their consent. Not only was that morally and legally reprehensible, but Bollaert also ran an online reputation rehabilitation website. He would essentially extort the victims by saying that if they paid money to his reputation website, he would contact YouGotPosted.com to remove their photos. He never disclosed that he ran both sites. Bollaert was playing both sides and

was eventually arrested. His criminal prosecution was the first of its type for revenge porn. He was eventually sentenced to 18 years.

What was interesting was that Bollaert attempted to use the Communications Decency Act from the 1990s as a defense. That Act protects Internet service providers as long as they are not content providers. That is Internet and legal mumbo jumbo for "If you just host the website, you will not get in trouble." Here, however, Bollaert did more than merely host the site; he created the website and invited people to upload the photos. These cases are on the cutting edge of the law as the law attempts to catch up with the technology.

It was an eye-opening experience to learn about these new types of crimes. Many thanks to Judge Mills' group for freaking everybody out.

The Robert G. McGrath American Inn of Court is now accepting applications for its September 2015 - June 2016 year. Also, we will be having a summer mixer on the evening of July 22, 2015.

If you are interested in applying for RGMAIOC membership or attending our summer mixer, please contact Patricia Kelly at patriciakelly@pacbell.net.

***Matthew B. Talbot**, Esq., is an Elder Law attorney in Walnut Creek. His practice specializes in Estate Planning, Trust/Probate Administration, Trust/Probate Litigation, Conservatorships, Guardianships, Elder Abuse and Medi-Cal matters. Matthew is on the Executive Board of the Inns of Court. You can reach him at matthew@matthewbtalbot.com or (925) 322-1763.*

The (Privacy) Darwin Awards

Monday, June 01, 2015

In the spirit of this issue and its focus on how the Internet has eroded our sense of (and right to) privacy, below we share some of our nominations for best use of online media. Enjoy.

Crime Boasting

Bragging about your crimes on Facebook, including drunk driving, is generally not a great idea.

And how about this dynamic duo who robbed an Internet cafe—after they had logged into Facebook, but not logged out.

If the police are using social media to find you … don't post in the comments.

Job Bashing

If you just got a job at a day care center, and you really need that job, don't post about how you hate children.

Social Breach

When you enter into a confidential mediation settlement, remember to advise your clients that "confidential" means don't tell anyone—especially an oversharing teenage daughter who likes to post everything on Facebook.

Video Bust

Posting a "brag" video on YouTube is a sure-fire way to make sure you don't get caught. Not.

Instagram Banking

This one gets multiple entries. Not only did he (a) take a picture of his ransom note, and (b) record himself handing it to the cashier, he also (c) posted both on Instagram. As if that is not enough to qualify him, he maintains his innocence claiming "asking for money isn't a crime" and it was the teller's mistake when she gave him the money.

Bar Soap: June 2015

Monday, June 01, 2015

Admittedly, I have been remiss in preparing this Bar Soap column. Many things of interest have arisen within the past two months, and I am hopeful I can report on all of them, so let's get started.

The April Welcome Celebration for our new Bar Association Executive Director, **Theresa Hurley**, was a great success. Many thanks to the Brown, Church & Gee law firm for hosting that wonderful event. I was most impressed with all the new young faces present. That, of course, means the CCCBA continues to be a dynamic and ever evolving organization; nothing stale about it.

It was also wonderful to see another generation taking leadership, as I chatted with the new Board President, **Nick Casper**, and with his father and former president, **Stan Casper**.

My separate article on Coroner's Inquests in our county was well received. I have gotten many questions from readers inquiring as to the identity of the official coroner in Contra Costa. Sorry I failed to mention it in the article. As in most counties in California, the coroner is also the sheriff. So our Sheriff Coroner is **David Livingston**. Sheriff Livingston is also a licensed attorney in the state of California and a member of the Contra Costa County Bar Association.

It always warms my heart to report on prestigious awards earned by local Contra Costa attorneys. Our own **Andy Schwartz** recently became a Fellow of the American College of Trial Lawyers, one of the premier legal associations in America. For trial lawyers, it is as prestigious an honor as one can get. His induction ceremony took place in Key Biscayne, Florida. Rumor has it that he had to purchase a tuxedo for the event. Congratulations, Andy, on the very high honor.

And speaking of awards, a number of you have reported being honored as "Super Lawyers." In fact, **Harvey Sohnen** reported that he is the only Super Lawyer practicing employment law between the Caldecott Tunnel and the Lafayette border. And seriously, it is an honor to be named a Super Lawyer, so please let me know and I will mention it. **Natasha S. Chee** was selected for "Rising Stars for Super Lawyers." She is on the board of our Barristers Section.

Many local lawyers are on the move. I missed the Law Practice Management Series program entitled, “Look Before You Leap in Changing Law Firms,” but I am interested to hear if it had any effect on the moves.

Matthew Talbot is now at the Law Offices of Matthew B. Talbot. Another one of my former Ropers Majeski colleagues, **Adrian Driscoll**, is now at Murphy Pearson. **Jeffrey T. Thayer** recently made partner at DeHay & Elliston, LLP, in Oakland. Jeff is on the board of our Barristers Section. **James Wu** and **Claudia Castillo** have teamed up to form Wu Castillo, PC, specializing in employment law. **Gina Boer** has become a partner at Haapala, Thompson & Abern, LLP.

Robert M. Slattery has changed the direction of his legal career. After 40 years of trial work, he is now going to focus on his own practice of mediation, specializing in professional negligence cases. **Robin Pearson** was just elected as Vice Chair of the State Bar Council on Access & Fairness. Guichard, Teng & Portello is planning a move back to Walnut Creek by the end of June. I think the firm will be called Guichard, Teng, Portello & Portillo; keep a look out.

And seemingly all too often, I report on the loss of members of the CCCBA. **Tom Henze**, a former Walnut Creek/Danville attorney and former member of our local bar passed away in Oregon, where he had retired. **Dick Grossman**, a local attorney and a former Walnut Creek police officer, passed away last December.

And an attorney a little closer to me, **Forrest Plant**, a longtime fixture in the Sacramento legal community at Diepenbrock, Wulff, Plant & Hannegan, and a former president of the California State Bar Association, passed away recently. His father was the first city attorney for Davis, having put together the articles of incorporation for that city. My middle name is Plant, just to let you know the connection.

And once again, I would like to mention the Contra Costa County Mock Trial Competition. The yearly event took place a couple of months ago. The high school teams take over the Bray Courthouse for a number of evenings during the week. It’s amazing to see the skill and intensity of the teams.

I was honored to act as a judge for the competition. I was also very happy to see the large number of volunteers from the legal community and the local bench who participated as judges, mentors and evaluators. Volunteer next year if you can.

I am in the process of preparing another “Civil Jury Verdicts” column. As you have probably noticed, those columns have become few and far between. I am simply not getting the reports as I once did. Believe it or not, when I first began writing that column, it came out every month. I just received enough reports to make it on its own. Occasionally, as you may have noticed, I include jury verdicts in this Bar Soap column.

And speaking of trials, I tried a case in Santa Clara County, representing business clients who were born and raised in China. One of my clients, Rebecca Li-Huang, wrote a book about the experience, and it just was named as an honorable mention at the San Francisco Book Festival. The book is entitled “Green Apple Red Book: A Trial and Errors.” It is an interesting and fun read, but I must say, I do not recall all the excerpts in which I am mentioned.

I would be remiss if I did not mention a topic which pains many of us who were former

deputies as well as the current members of the local District Attorney's Office. I have followed the case in the papers and occasionally through PACER in the U.S. District Court. The *Michael Gressett v. Contra Costa County, et al* case now appears to be at an end. Summary judgment was granted in its entirety. It is a sad saga for all parties.

Please keep those cards and letters coming or email me at mguichard@gtplawyers.com.

Women’s Section 2015 Wine Tasting & Silent Auction [photos]

Monday, June 01, 2015

The Women's Section Annual Wine Tasting and Silent Auction was held on Thursday, April 23, 2015.

Thank you to all supporters! Proceeds benefitted the Hon. Patricia Herron and Hon. Ellen James Scholarship Fund.

Photos from the event are below, with more photos available on our Facebook page.

[gallery columns="4" ids="10346,10347,10355,10348,10345,10349,10350,10351,10352,10353,10354,10356"]

Bench/Bar BBQ & Softball [photos]

Monday, June 01, 2015

On Saturday, May 16, 2015, the Contra Costa Superior Court and the CCCBA came together to enjoy some burgers, dogs and a little softball in between bites.

Below are photos from the event. To see more photos, please visit our Facebook page.

[gallery ids="10337,10338,10339,10340,10341,10342"]

Don't Miss the 2015 Law Practice Management Series

Monday, June 01, 2015

Get your MCLE credits with the 2015 Law Practice Management Series


LAW PRACTICE MANAGEMENT SERIES 2015

Our next program is on **June 17:** Everyone's Doing It: The Explicit Effect of Implicit Bias.

This year's six-part series will take place on the third Wednesday of each month through October 2015 (no program in August) from 4:30 - 6 pm at JFK University in Pleasant Hill.

All programs will be for MCLE credit and cost only $20 per program for members ($10 for law students)! Light refreshments will be provided. We hope you will join us!

Previous programs can be viewed on our MCLE Self-Study page.

For more information, please contact Liz Galliett at (925) 370-2540 or lgalliett@cccba.org or go online to the CCCBA Event Calendar to register.

Target Your Search with CCCBA's Job Board

Monday, June 01, 2015

Whether you are hiring or looking for a job, our **Job Board** is a great place to target your search. CCCBA members receive special pricing to post jobs, while job seekers can post resumes and create job alerts for free!

Member Comment:

"We have used the CCCBA job board with success. It is a great resource for employers since (1) there is no high priced recruiter fee (which can typically range from 20% – 30% of salary); (2) the cost to advertise is less expensive or comparable to publications or websites which have legal classifieds; (3) you get a self-selected group of applicants for your practice and geographical area. It is not a cattle call. We received quality applications from good, solid candidates. The CCCBA job board should be on the list of places where you advertise. Be sure to tell your HR manager or office administrator about this resource. You get a great bang for your dollar."

- Audrey Gee, Partner, Brown Church & Gee, LLP

Are you hiring?

The best and brightest legal professionals in Contra Costa County are our members. Access this targeted and qualified pool of talent by advertising your jobs on our career center.

- Easily post jobs.
- Search the Resume Bank and pay only for resumes of job seekers interested in your position.
- Access highly-qualified, professional candidates.
- Set-up pre-screen filters to deliver the best candidates.
- **CCCBA Members receive special pricing. Just use coupon code CCCBA-JOBS and receive a 30-day job posting for just $99!**

Post your jobs at: jobs.cccba.org.

Looking for a job?

Connect with employers who are looking for YOUR skills and experience.

Tired of searching through hundreds of random job postings to find your next opportunity? Your search is about to became a whole lot easier. Visit the CCCBA's Job Board.

- Find targeted opportunities.
- Post your resume anonymously.
- Create job alerts.

And do it all in less time than it takes to search through job postings on the mass job boards. Visit today at jobs.cccba.org.

Questions?

The CCCBA Job Board is powered by **YourMembership**, a company specializing in building targeted career centers for niche markets, like Bar Associations. If you have any questions about posting a job or creating a job seeker account, please contact Dawnell Blaylock at dblaylock@cccba.org.

Welcome to Our Newest Members!

Monday, June 01, 2015

Please welcome our newest members that have recently joined the CCCBA:

Jason Burgess Maria Oropeza Margaret Cole John Pearson Rachel Ehrlich Mujdah Rahim Sterling Elmore Nicole Saputo Gregory Feldman Randall Schram Heather Hoekstra Michael Shepherd Cris Jarrell Gina Steele Diana Kaempfer Ashley Stefan Michael Meinert Peter Sumulong Cody Nevels