Prescription Medication and the Workplace .............................. 2

What Happens When a Computer Containing Patient Medical Information Is Stolen From a Hospital ................................. 4

When Cyber Insurance Is Not Enough For a Data Breach ...... 6

Google Maps are Great, But They Come With a Potentially Hefty Loss of Privacy ................................................................. 8

Beware of the Blog – and the Lawsuits Which It May Cause .... 10
While everyone is familiar with the rule that employers have the right, under certain circumstances, to test their employees for illegal substances, it is less clear whether employers may test their employees for the legal use of prescription drugs. This can be problematic because disclosure of prescription medication use can be indicative of wider medical issues protected by an employee’s privacy rights. However, the employer also has an interest in preventing workers in safety-sensitive positions from working while under the influence of these legal substances. So in a balancing test of competing legal interests, whose interests are paramount?

As a basic principle, California is one of the few states whose Constitution includes a right to privacy. California courts have held that this right is implicated by employee drug testing, but that does not mean it is illegal to conduct employee drug testing. Instead, the courts have held that an employer’s right of testing is determined on a case-by-case basis, balancing the employer’s reasons for testing against the intrusion it imposes upon the employee or applicant.

Published court opinions in California have held generally that employers may require employees to pass a drug test as a condition of ongoing employment. As long as an employer tests all applicants for particular job positions and does not single out certain applicants based on protected characteristics (such as race or disability), courts have upheld this type of testing. California courts generally also have allowed testing of specific employees based on “reasonable suspicion,” where an employee has exhibited physical or behavioral symptoms or reactions commonly attributed to the use of controlled substances or alcohol.

Random testing of employees is a more difficult issue to adjudicate, although courts have upheld random testing for very safety-sensitive positions, e.g., where the operation of heavy machinery is more likely to put persons at risk should the employee work “under the influence.”

Situations arise, whether in random testing or selected testing, when some prescribed medications turn up in drug test results. This can become a very challenging issue because what qualifies as a prescribed medication versus an illegal substance is sometimes difficult to define. For example, some drugs which ordinarily are considered illegal, such as opiates, can be prescribed legitimately for certain medical conditions. If a job applicant is turned down for an employment position because of a positive finding for a prescribed drug, the prospective employer could be liable since prescription medication is considered “medical information” and thus subject to a higher sense of privacy than illegal drug use. Accordingly, prescription medication usage should be treated differently than illegal drug and alcohol usage, due to the privacy interest in the medical information that can be gleaned from it.

It is important to note that California follows the “compassionate use” law, which allows residents to use marijuana for medical purposes, although state law requires users to obtain a medical doctor’s written authorization to use marijuana. A patient who has a valid prescription may not be prosecuted under state law for crimes relating to the use, possession, or cultivation of a certain amount of marijuana. (State law does
not preclude any prohibitions imposed by Federal law.) However, the California Supreme Court has held that an employer may refuse to hire an applicant who tests positive for marijuana, even if the drug is legally prescribed for a disability. Hence, it seems that there is always an exception to the general rule.

CAVEAT: THE FOREGOING DOES NOT CONSTITUTE LEGAL ADVICE. PLEASE CONSULT AN ATTORNEY FOR INDIVIDUAL ADVICE REGARDING INDIVIDUAL SITUATIONS.
Privacy breaches and cyber threats continue to generate substantial litigation, with what often appears to result in an ever-expanding scope of liability. It is therefore good to see a case that tries to limit the reach of privacy breach liability.

The recent case of Eisenhower Medical Center v. Superior Court 226 Cal.App.4th 430 (filed May 21, 2014) involved a case against a hospital under the Confidentiality of Medical Information Act (CMIA), codified as California Civil Code Section 56 et seq. A computer was stolen from the Eisenhower Medical Center (EMC) that contained an index of over 500,000 persons to whom EMC had assigned a record number. The information on the computer included the person’s name, medical record number (MRN), age, date of birth, and the last four digits of the person’s Social Security number. EMC provided notice to the individuals informing them of the theft, and several of the individuals whose names were on the index filed suit against EMC.

EMC moved for summary judgment or adjudication, contending that the information on the computer did not constitute disclosure of medical information within the meaning of the CMIA, which requires disclosure of “individually identifiable information … regarding a patient’s medical history, mental or physical condition, or treatment.” Civil Code Section 56.05(j), formerly 56.05(g). Further, the statute defines “individually identifiable” as medical information that “includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient’s name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual’s identity.” EMC conceded that the information on the stolen computer contained individually identifiable information, but asserted that it did not contain information regarding the patient’s medical history or condition.

The plaintiffs contended the mere fact that a person’s name was on the index revealed that he or she was a patient, and that constituted a release of medical history. The trial court agreed, and denied EMC’s motion for summary adjudication. The Fourth District of the California Court of Appeal agreed with EMC, and issued a peremptory writ of mandate directing the Superior Court to set aside its order denying summary adjudication as to the cause of action for breach under the CMIA.

The decision by the Court of Appeal was based on fundamental rules of statutory construction, and courts look to the “plain meaning of the statute unless it would be repugnant to the obvious purpose of the statute.” Eisenhower, supra 226 Cal.App.4th at 435, citing Lungren v. Deukmejian, 45 Cal.3d 727, 735 (1988). The Court found that the plain meaning of the statute, in referring to “medical information,” did not mean just any information regarding the patient, but must contain the patient’s “medical history, mental or physical condition, or treatment.” Id. The Court held that this does not encompass merely demographic or numeric information without the actual medical history, diagnosis or care given to the patient.
The Court cited several other statutes in which the California Legislature has made a distinction between demographic information and medical information, including several Penal Code sections, as well as Civil Code Section 1798.82, the Customer Records Act (CRA), which requires notification in the event of a breach. EMC’s position was that there is no showing that mere assignment of a medical record number indicates a person has had medical treatment; even if it can be assumed that the person may have been treated at EMC, that fact alone is not “medical information” under the definition of Civil Code Section 56.05. The Court of Appeal agreed with the hospital and directed the Superior Court to grant the motion for summary adjudication on this issue.

While computer theft, and electronic privacy breaches are still very much in the forefront of today’s legal scene, not all computer theft is actionable, if there is no true damage as a result.

CAVEAT: THE FOREGOING DOES NOT CONSTITUTE LEGAL ADVICE. PLEASE CONSULT AN ATTORNEY FOR INDIVIDUAL ADVICE REGARDING INDIVIDUAL SITUATIONS.
WHEN CYBER INSURANCE IS NOT ENOUGH FOR A DATA BREACH CLAIM

© Sandra Calin
Partner, Kramer, deBoer & Keane, LLP

As Target recovers from its data breach incident last year, more and more companies are realizing that a potential data breach of their computer systems is a very real possibility, and that the attendant costs can be astronomical. Is there insurance that will cover such a breach? The short answer is yes, there is insurance, but no, it might not cover all of the losses associated with a breach.

Given the sophistication of hackers today, it is a reality that virtually every data base can be breached, even in the most vigilant of companies. Corporate executives and small business owners alike are realizing that their security and technology departments must implement reasonable safeguards for protecting data and sensitive customer information at every level of the organization. The unpleasant alternatives include expensive litigation and severe compromises of a business’s goodwill.

Because it suffered one of the largest and most noteworthy recent breaches, and a lot has been written about it, let’s take Target as an example. What was the nature of the loss? What costs continue to be associated with the aftermath of the breach? How much of it, if any, might insurance cover?

According to regulatory filings, Target has incurred some $88 million in breach-related expenses, and expects that its insurance will only cover about $52 million of that amount. To make matters worse, there are less tangible but nonetheless real losses too. Target’s profits decreased drastically, and the damage to its brand is immeasurable. How do you evaluate such a loss? Following the breach, Target promised its customers that it would quickly adopt more secure technology to prevent a similar breach in the future, but the cost of those measures will likely be very high, and not all of them might be insurable. Some analysts have forecast that Target will suffer $1 billion in losses as a result of the attack, much of which arguably will not be covered by insurance.

So once a breach occurs, what can the victim company do? Whether it is a large organization like Target or someone much smaller, the majority of jurisdictions in the United States mandate that everyone must begin by immediately notifying all customers who could be affected by the breach. The operative California statute is Civil Code Section 1798.82, and it is comparable in scope to similar statues which are found in other jurisdictions.

Civil Code Section 1798.82 requires that disclosure must made “in the most expedient time possible and without unreasonable delay.” That means the immediate issuance of letters, e-mails, and public notices, all of which can cost the company millions of dollars in processing expense. In addition, as did Target, the breached company can set up call centers to answer customers’ questions, and pay for free credit monitoring for those customers who may have been affected. These costs are typically covered by insurance, but not always necessarily so.

So what can a company do to protect itself? The good news is that more and more insurers are writing cyber insurance policies to cover up-front notification/remedial costs following a breach. However,
companies need to be aware that these policies often have high deductibles, and they are unlikely to cover many intangible losses that can be expected as a result of a cyber-attack. This is important to note because intangible losses, such as stolen trade secrets and damage to reputation, tend to be very costly and damaging to a business’s ongoing operations.

Insurance products continue to evolve for these types of risks. One large insurer recently expanded the scope of its cyber risk policies to cover physical risks, including bodily injury and property damage. But we should not assume that every policy can cover every possible type of cyber-related loss. There is a great likelihood that even the policies with the broadest available coverage might still not afford complete coverage.

Hence, every company, whether large or small, should establish a contingency plan in the event of a cyber-attack. While that plan may include insurance, every company is well-advised to set aside financial reserves that can fund notification/remediation measures if a breach occurs which results in uninsured losses.
GOOGLE MAPS ARE GREAT, BUT THEY COME WITH A POTENTIALLY HEFTY LOSS OF PRIVACY

© Sandra Calin
Partner, Kramer, deBoer & Keane, LLP

Who remembers the old Thomas Guide? That was my bible years ago for finding my way anywhere while driving. I had a Thomas Guide for every county in Southern California, and some in Northern California too. Then along came the Internet, Mapquest, Yahoo Maps, and of course, Google Maps. Google soon launched its Street View feature, and all of a sudden, you could see a street-level photograph of your destination.

Just how does Google manage to get those Street View photographs? Apparently, the photographs are captured using cameras mounted on vehicles that are owned by Google, and photographers take a series of still pictures as they drive along public roads. More recently, Google also equipped its cars with Wi-Fi antennas and software that collects data transmitted by Wi-Fi networks in nearby homes and businesses. This equipment recorded basic information about those Wi-Fi networks, such as the network’s name, router information, signal strength and whether the network was encrypted.

But apparently the antennas and software collected more than just basic identifying information. The also collected and stored data transmitted over unencrypted connections such as personal email addresses, usernames, passwords, and related documents. In May 2010, Google admitted that its Street View vehicles had been collecting such data from unencrypted Wi-Fi networks. It publicly apologized, grounded its vehicles, and made inaccessible the data that had been collected.

Several putative class action lawsuits were filed and eventually consolidated in Federal Court in San Francisco, where a Complaint was filed in the U.S. District Court, alleging claims against Google under the Federal Wiretap Act, 18 U.S.C. Section 2511, California Business and Professions Code Section 17200 and various state wiretap statutes. The District Court denied Google’s motion to dismiss and the Ninth Circuit Court of Appeal affirmed the District Court’s decision in Joffe v. Google, Inc., 729 F.3d 1262 (2013), as amended at 2013 WL 6905957 (Dec. 27, 2013).

The Ninth Circuit U.S. Court of Appeals found that Google’s acts fell within the purview of the Wiretap Act, which imposes liability on a person who “intentionally intercepts … any wire, oral, or electronic communication” but subject to several exemptions. One of the exemptions is for intercepting electronic communications “made through an electronic communication system” if the system is configured so that it is “readily accessible to the general public.” Further, 18 U.S.C. Section 2510(16)(A) defines “readily accessible to the general public” as communication that is not encrypted. Google argued that it is exempt from liability pursuant to this exemption.

However, the Federal trial court disagreed, and so did the Federal appellate court, which held that Google is liable because the data acquired by Google which was transmitted over an unencrypted Wi-Fi

---

1 18 U.S.C. §§ 2511(1)(a) and §2511(2)(a)-(h).
network is not “readily accessible to the general public” under the ordinary meaning of that phrase. Though unencrypted, the Wi-Fi transmissions are geographically limited and do not travel very far beyond the home or office where they originate. Nor do they constitute a “radio communication” under 18 U.S.C. Section 2510(16). Google was only able to obtain the data because its vehicles passed by the street outside each plaintiff’s home, using sophisticated equipment not otherwise available to the general public.

The Court held that even if members of the general public occasionally connect to a neighbor’s unencrypted Wi-Fi network, they do not typically intercept, store and decode data transmitted by other devices on the network. Therefore, Wi-Fi communications are sufficiently inaccessible that Google’s act of collecting this data fell within the Wiretap Act.

Google can still send its vehicles around city streets to take photographs, but the vehicles cannot collect data emanating from personal unencrypted networks. One wonders, however, how much data Google has on us, and what it could ultimately do with the information.

CAVEAT: THE FOREGOING DOES NOT CONSTITUTE LEGAL ADVICE. PLEASE CONSULT AN ATTORNEY FOR INDIVIDUAL ADVICE REGARDING INDIVIDUAL SITUATIONS.
BEWARE OF THE BLOG – AND THE LAWSUITS WHICH IT MAY CAUSE

© Mark C. Phillips
Partner, Kramer, deBoer & Keane, LLP

Several years ago I handled a very difficult type of property damage claim. The homeowners chose not to litigate their claim in a court of law. They chose instead to prosecute the claim, without an attorney, in the court of public opinion through a very aggressive and inflammatory series of blog posts. Everything appeared in the painfully slanted blog. The blog posts ended only when the claim was resolved.

More and more claims are being advanced through social media, which creates a challenging issue for bloggers and those who must deal with them. State law can protect litigants from being sued for slander and defamation under the so-called litigation privilege, so long as the inflammatory comment is contained within a pleading or other court-sanctioned document. A blog, however, does not meet that definition. Is the blogger therefore protected from a slander or defamation suit when discussing a claim for damages?

The U.S. Ninth Circuit Court of Appeals, which is a Federal appellate court located in California, Nevada, Oregon and several other Western states, decided in January 2014 that “it depends.” The litigation privilege available under state law does not apply in federal question cases, but First Amendment free speech protections might apply unless there is proof of fault and actual damages. If fault and actual damages are proven, then the blogger may be liable.

In Obsidian Finance Group, LLC v. Cox, 740 F.3d 1284 (9th Cir. 2014), a business adviser was hired to assist an Oregon-based company which was contemplating bankruptcy. The business advisor’s owner was appointed the client’s bankruptcy trustee to marshal the client’s assets for the benefits of claimants. An observer published blog posts on several websites that she created, accusing the business advisor and trustee of various illegal activities. A cease-and-desist letter was sent, and ignored. A defamation lawsuit followed.

The U.S. District Court located in Portland, Oregon ruled that all but one of the blog posts was a constitutionally protected personal opinion. Most of the blogs used such phrases as “deceit on the government,” “money laundering” and “tax crimes” were thrown around. The District Court held that such phrases were merely “figurative and hyperbolic language” and could not be proved either true or false.

The District Court did allow trial on one factually specific blog post, that the court-appointed bankruptcy trustee had committed tax fraud while administering the assets of a company undergoing Chapter 11 reorganization. The jury awarded seven figures to the business advisor and owner in compensatory damages. The key issue was whether the blogger was a *bona fide* journalist and the plaintiffs were *bona fide* public figures, such that the First Amendment required the plaintiffs to prove the blogger had acted with either negligence or actual malice. The court decided otherwise, and also denied the blogger’s Motion for New Trial on this issue.

On appeal, the Ninth Circuit noted the historic evolution of First Amendment law in cases where the plaintiffs are public figures versus private individuals. Plaintiffs who are public figures must prove actual malice, i.e., that the defendant published the defamatory statement “with knowledge that it was false or with
reckless disregard of whether it was false or not.” Private individuals who sue for defamation need only prove negligence. **What makes this case unique is that none of the earlier cases discuss blog posts.**

Historically, First Amendment protections have been afforded to the institutional press but that does not mean the press is entitled to legal immunity in all defamation lawsuits. Whether a professional journalist or a blogger, “the line between the media and others becomes far more blurred.” The evidentiary standard for proving a defamation case does not rest upon whether the defendant is a *bona fide* journalist or blogger, but whether the plaintiff is a public figure and the public importance of the statement at issue.

The Ninth Circuit determined that the blog post in this case constituted a matter of public concern. It was not a matter of private concern or pertinent only to a specific business audience: it was published to the public at large and could not be dismissed as a form of advertising. However, a bankruptcy trustee is not considered a public figure: he or she simply substitutes for the debtor-in-possession. Thus, this case involved a matter of public concern but not public figure. The plaintiffs, therefore, were required to prove only negligence against the blogger, not the higher standard of actual malice, because they were not considered public figures. A finding of negligence requires a finding of damage too, hence the plaintiffs were required to prove that they suffered actual damages as a result of the blog post.

Statements of opinion are not actionable. In order to avoid defamation as an opinion, an otherwise offensive communication must meet all three prongs of a three-part test for whether the communication is truly an opinion:

- Whether the general tenor of the entire work negates the impression that the defendant was asserting an objective fact;
- Whether the defendant used figurative or hyperbolic language that negates that impression; and
- Whether the statement in question is susceptible of being proved true or false.³

One of the many lessons from this case is that blogs may not be as innocent as they seem. Blog posts are not necessarily protected speech under the First Amendment, and they can generate liability for the blogger. As a general rule, think twice (or even thrice) before posting anything that you do not want to see displayed as an exhibit before the jury.

---

³ *Obsidian Finance Group, LLC v. Cox*, 740 F.3d 1284, 1293 (9th Cir.2014).

**CAVEAT:** THE FOREGOING DOES NOT CONSTITUTE LEGAL ADVICE. PLEASE CONSULT AN ATTORNEY FOR INDIVIDUAL ADVICE REGARDING INDIVIDUAL SITUATIONS.