Computers, Social Media and Legal Ethics

By

Chuck Sevilla

Presented December 14, 2013 to the
California Attorneys for Criminal Justice
Updated August 10, 2015

Law Office of Charles M. Sevilla
1010 Second Avenue, Suite 1825
San Diego, California 92101-4902
619 232 2222 Chuck@charlessevilla.com

CONTENTS

Introduction

We live in an incredibly fast moving society. No creations have sped up our lives more than the computer, internet and social media. Because nearly everyone is using all three, including our clients, we must be alert to the many issues raised by these techniques of human communication. The California Business & Professions Code, State Bar Ethics Opinions, and the Rules of Professional conduct require it. To comply, we must have a basic understanding of the hardware and software, and their vulnerabilities, that we employ in our daily work. Further, we must advocate privacy protections against the onslaught of new technology.

The legal and ethical challenges to new technology are enormous. Privacy rights are on the line (pun intended) every time we use our computers, tablets and smart phones. For example, the Ninth Circuit recently decided Joffe, et al v. Google (9th Cir. 2013) 729 F.3d 1262, which revealed that from 2007 to 2010, Google was sending its Street View cars into neighborhoods to photograph homes for Google Maps. However, it was also collecting "payload data" from the homes through their unsecured Wi-Fi networks. This enabled Google to grab everything ranging from personal emails, usernames, passwords, videos and documents. In defense to the civil lawsuit brought by a number of victims who claimed wiretap violations, Google defended by arguing that unencrypted data transmitted over Wi-Fi networks is readily accessible to the general public because the hardware used to make the intercepts can be purchased by anyone and the software is available on the internet. The Circuit rejected the arguments and thus making Google liable for wiretap violations. However, the fact that the "sniffing" equipment is out there freely available to cyber crooks to buy and use should serve as a warning about the need to protect one's electronic devices.

The Google case has implications about our ethical duties to maintain client confidences in that it *may* mean that it is *not* negligent to use a work laptop at a Starbucks, the airport or any location that offers free, open, unprotected WiFi. This is because it may be reasonable to assume that illegal wiretaps are not taking place there. Maybe. While it may be ethical to use work laptops are such locations, it still is unwise to do so given the ease with which crooks can intercept and invade your e-space.

Another important Google case is now in litigation in Santa Clara. There, the plaintiffs allege that Google's practice of automatically scanning e-mail messages and showing ads based on the contents of the e-mails, violates wiretapping laws. Google argued that non-Gmail users have no expectation of privacy when corresponding with Gmail users and that Gmail users consented to the Google's interceptions. Further,

Google argued that non-Gmail users communicating with Gmail users knew that their messages could be read. Federal Judge Lucy H. Koh, rejected these arguments and denied Google's motion to dismiss the case. Claire Cain Miller, "Google Accused of Wiretapping in Gmail Scans," Oct. 1, 2013 New York Times, http://tinyurl.com/m74umt6.

Case law thus seems to be evolving to set barriers against these intercepts, intrusions and outright hacking. *See* Jardines v. U.S. (2013) 568 U.S. __, 133 S.Ct 1409 (taking a drug-detecting dog to the front porch for a sniff test is a search and requires a warrant); U.S. v. Jones (2012) 565 U.S. __, 132 S.Ct. 945 (police installation of GPS[1] tracking devices on a car and then tracking it for 28 days constituted a search under the Fourth Amendment); Kylo v. U.S. (2001) 533 U.S. 27, 121 S.Ct. 2038 (use of thermal imaging device to scan home to determine if the heat coming from it was consistent with the use of high intensity lights used in a pot grow was a search and presumed unreasonable without a warrant); U.S. v. Cotterman (9th Cir. en banc 2013) 709 F.3d 952, 957 ("individual privacy interests in data on portable digital devices" is a basis for requiring reasonable suspicion for the forensic examination of a laptop seized at the border); U.S. v. Comprehensive Drug Testing, Inc. (9th Cir. en banc 2010) 621 F.3d 1162 (setting for guidance for search warrants to obtain electronic data); see U.S. v. Dreyer (9th Cir. 2014) 782 F.3d 416 ("The extraordinary nature of the surveillance here demonstrates a need to deter future violations. So far as we can tell from the record, it has become a routine practice for the Navy to conduct surveillance of all the civilian computers in an entire state to see whether any child pornography can be found on them, and then to turn over the information to civilian law enforcement when no military connection exists.")

On the other hand, criminal defense attorneys often seek evidence from social media but run into barriers from media organizations like Facebook. In Negro v. Superior Court (2014) 230 Cal.App.4th 879, the court held that a trial judge can order a civil litigant to give consent to a disclosure of Internet information to another party to the case.

I would like to tip my hat to the Electronic Frontier Foundation which is in the forefront of litigating these issues and educating us in the ever-changing area. They will provide assistance to us in dealing with these issues. It is hoped that the following diverse materials will assist you in coping with the practical, legal and ethical challenges we face in this swiftly changing era.

---

[1] In United States v. Katzin, 769 F.3d 163 (3d Cir. en banc 2014), the Court addressed an issue Jones left open whether the police must obtain a warrant prior to a GPS search and whether the conduct in this case can be excused on the basis of good faith. Answers: yes and yes.

Social Network Addiction and Your Next Case

By Charles Sevilla

Everyone is familiar with the widespread use of social networking and the electronics needed to access them. Everyday we see people with their heads down walking busy streets, or worse, driving, while texting on their iPhones or Droids, checking email, or posting the latest news about their busy day.

This phenomenon is a major cultural shift in the way we live and communicate. Today, people are in constant touch with their friends and others (including, like it or not, enemies) by their daily postings revealing all sorts of data about themselves. Naturally, if such a social movement affects the universe, it inevitably affects the legal world. And it has. In a big way.

The cyberworld is far too immense for a discussion of all the legal issues that arise in it. The purpose of this paper is to suggest ways for counsel to talk to clients, witnesses and staff about their uses of cyberinformation and alert practitioners to issues that will undermine a case and a client.

Social Network Addiction. Many users are addicted to their social media and electronics. Psychologists like Dr. Michael Fenichel have popularized the notion of a Facebook Addiction Disorder (FAD) -- that is, an obsession to spend so many hours of the day on Facebook that one's life is adversely affected. Such addiction affects our clients.

Problem Examples. The varieties of mischief clients and witnesses can create for themselves on the internet or with cell phones and other electronic equipment are almost endless. A few include:

-a juror contaminates the verdict in a long trial by daily posting on Facebook or Twitter about how the case is going;

-a trial witness is destroyed on cross-examination by having her testimony exposed as a lie by her Facebook postings made the previous day;

-a client is discovered running an illegal cocaine business through Craig's List;

-a miscreant runs an anonymous (or so he thinks) libelous cybersmear campaign via webposts against a person's small business;

- a bully, using a fake social network profile, repeatedly attacks a person on that person's social network causing the latter to commit suicide.

All these things have occurred. Lawyers have a duty to be aware of the problems attendant to social networking. Many people cannot stop using their electronic devices to communicate about themselves no matter what the discouragement. It is thus immensely frustrating for judges who have instructed jurors not to use their electronics and discuss the case as it proceeds through trial only to learn post-verdict that jurors have done just that. Trials have been overturned as a result. New legislation attempts to address the problem.[2]

Lawyers need to take affirmative steps to make sure that the addiction does not corrupt their cases.

First Interview Checklist. When interviewing a new client (or a witness) inquiries must be made of the use of social media. Clients, and particularly younger ones, may see older attorneys as technological dinosaurs and tend to dismiss lawyerly admonitions. Thus, it is important to carefully explain the potential self-destruction that comes with misuse. The following list of suggested questions provides a start to client counseling. An explanatory introduction to these questions could begin with:

> *Because the internet could be a source of much public information about yourself, I need to know what presence, if any, you have there. Law enforcement routinely checks available resources on the internet to discover information about persons of interest. This has led to persons being criminally prosecuted simply based upon what they have placed on the internet, or perhaps what their friends have posted about them. Just as should not speak about your case, you must not post anything about it on social media, email, etc. To properly advise you, I need to know the following:*
>
> 1. Do you have a profile on a social network like Facebook, Twitter, Linked-in, MySpace, Google Plus, etc.? Is it in your name? How many such profiles do you

[2] Effective January 1, 2012, California law states that jurors must be instructed not to conduct research, disseminate information, or converse by any form of electronic or wireless communication. Penal Code section 1122(a)(1); CCP section 611. Violations are punishable by civil or criminal contempt. CCP section 1209(6); Penal Code section 166(6).

have? Are they it open to the public? What is posted? Where else do you post your communications? Have you commented on articles, blogs, or pictures on other people's social media sites?

2. Do you have your own website? How long have you had it? When did you first launch the site?

3. Do you have a blog? What do you post there?

4. Do you post material on YouTube? What exactly?

5. Do you buy or sell on eBay, Craigslist, or similar services?

6. Does your cell phone have video? Do you have a Flip Video or other similar recorder? Where is the content stored? Do you upload any of it to the net (i.e., YouTube)?

7. Do you email from a computer, Blackberry, smart phone, iPod, iTouch or other device? Do you use Skype or Gchat? FaceTime? Instant Message?

8. Do you text message from your cell phone?

9. Do you use LimeWire or similar peer-to-peer programs? Why?

10. On what media do you store files or photos: a PC, Mac, laptop, PDA, DVD, CD, Compaq Flash cards, or do you backup files to an internet site DropBox, iCloud, Mozy or similar internet resources?

Caveat. Depending on the answers, each of the above questions may trigger follow up questions. And this raises an important point. What if clients tell you they post material on their website or blog that may well have evidentiary value to the case? What if this material may undermine the client's credibility or implicate the client in criminal activity. What does one advise a client? If the social media site has obvious harmful "evidence" on it, counsel surely cannot advise taking down the material without

running afoul of ethical[3] and legal[4] mandates about destroying evidence. In one case, an attorney was fined $542,000 for telling his client to "clean up" his Facebook page and then lying about it. (Allied Concrete Co. v. Lester (2013) 285 Va. 295, 303.)

All counsel can do is advise, as stated in the introduction to the checklist, that social network surveillance occurs continuously in the cyberworld. Counsel should also strongly advise the client never to discuss the case with others in emails, blogs, or network sites; *i.e.,* outside the confines of the attorney client privilege.

First Interview Warning About Confidentiality. Any discussion with others about the case and particularly about communications with counsel, be they verbal or in writing (*e.g.,* email, blog or social network posts) can destroy the confidentiality of that communication and thus the attorney client privilege. This means the communication is fair game for collection and use by outsiders. As one court stated: "When a client reveals to a third party that something is 'what my lawyer thinks,' she cannot avoid discovery on the basis that the communication was confidential."[5]

The client should also be warned not to attempt to contact, photograph or harass adverse witnesses. Even anonymous email contacts or Facebook postings can be discovered both technologically and legally.[6] Such contacts, if threatening or harassing, may also be criminal. (*E.g.*, In re Rolando S. (2011) 197 Cal.App.4th 936 [the defendant accessed the victim's Facebook account, altered her profile, and posted obscene messages and comments purporting to come from her; held, this constituted identity theft in

---

[3] California Rule of Professional Conduct 5-220 states: "A member shall not suppress any evidence that the member or the member's client has a legal obligation to reveal or to produce."

[4] See People v. Meredith, 29 Cal.3d 682 (1981)(counsel cannot deprive the prosecutor of evidence of a crime found and retrieved by a defense investigator); Calif. Penal Code section 135 makes it a misdemeanor for a person who knows that material is about to be part of an authorized investigation destroys or conceals it.

[5] Lenz v. Universal Music Corp. (N.D. Cal. 2010) 2010 WL 4789099; 2010 U.S. Dist. LEXIS 125874. Note: this case involves opposing counsel getting a discovery order from the court for such communications.

[6] O'Grady v. Superior Court (2006) 139 Cal.App.4th 1423, 1446 ("where a party to the communication is also a party to the litigation, it would seem within the power of a court to require his consent to disclosure on pain of discovery sanctions.")

violation of Penal Code section 530.5(a) and also violated section 653m, subd. (a) by using an electronic communication device to contact another person with obscene language and an intent to annoy].)

Further, if the client uses computer shareware such a LimeWire, which opens access to the computer to anyone in the cyberworld, there is no confidentiality about *anything* on the computer. Such publicly accessible file-sharing computer programs are deemed the same as having a website open to the public. There is no expectation of privacy in such computers.[7] Clients should be instructed not to use such shareware because all communications by email with counsel will be open for public inspection and may destroy the confidentiality of those communications. Also, the typical use of such shareware is to violate copyrights by downloading as music, TV shows and movies, all of which are illegal.

Investigation. Whatever attorneys cannot do, the same rules also apply to staff, hired experts and investigators. We have a duty to make sure they all understand the rules.[8] One of the obvious investigative temptations is for the investigator to "friend" an adverse witness on Facebook. Is this permissible? Assume the investigator truthfully identifies himself but does not reveal that the purpose of the "friendship" is to gather information about the witness on a pending case. Several bar associations, including San Diego's, have found this practice unethical.[9]

There are also legal problems with such an investigative tactic. Penal Code section 1054.8 says that witnesses whose names have been disclosed in formal discovery in a criminal case cannot be questioned without the defense interviewer complying with disclosure requirements of the statute. This law has obvious application when contacting such witnesses via a social network or email.

---

[7] United States v. Borowy (9th Cir. 2010) 595 F.3d 1045, 1048.

[8] The Comment to Rule 3-110, Rules of Professional Conduct, states the duties of the rule "include the duty to supervise the work of subordinate attorney and non-attorney employees or agents." See also Crane v. State Bar (1981) 30 Cal.3d 117, 123) and Pincay v. Andrews (9th Cir. 2004) 389 F.3d 853, 856.

[9] The Philadelphia Bar Association Professional Guidance Committee stated that an attorney cannot ethically ask a third party [read investigator] to "friend" a witness on a social network. (Opinion 09-2, March 2009.) The San Diego Bar Association Ethics Committee agrees. It opined that a lawyer may not "friend" a represented party or, without disclosure, even an unrepresented person. (Ethics Opinion 2011-2.)

Generally, however, using internet tools to investigate witnesses can be very fruitful. Just "Googling" a name often provides valuable information and is permissible. A host of pay sites will drill deep into the cyberworld to gather even more information about a person. *See* Richard Demarest, "Using the Web (Visible, Invisible and Deep) to Investigate Government Experts," NACDL Champion (Nov. 2012), p. 14-24.

Conclusion. This article offers a view of some of the issues presenting themselves when the cyberworld meets the representation of clients. The message here is to make inquiries about client and witnesses use of the social networks, keeping in mind the above limitations of the law and ethical standards. Counsel's timely advice may forestall a client's silly conduct that comes back to damage the case.

ADDENDUM:

Steiner v. Sup. Ct. (Volkswagen) (2013) 20 Cal. App. 4th 1479 [An attorney's website advertised her success in two cases raising issues similar to those she was about to try in a products liability case. The trial court admonished the jury not to "Google" the attorneys or to read any articles about the case or anyone involved in it. Concerned that a juror might ignore these admonitions, the court ordered the attorney to remove for duration of trial two pages from her website discussing the similar cases. The Court of Appeal concluded that this constituted an unlawful prior restraint on the attorney's free speech rights under the First Amendment.]

Social Media & Jury Investigation Ethics

By Chuck Sevilla

This column is provoked by an interesting ethics opinion recently published by the New York City Bar Association's Committee on Professional Ethics, 2012-2, entitled "Jury Research and Social Media." In it, the Committee discusses important issues on attorney's duties with regard to social media investigations of jurors which I will discuss and correlate to California rules.

1. Attorneys cannot make *ex parte* communications with prospective or sitting jurors. This is a no-brainer. California Rule of Professional Conduct (RPC) states in Rule 5-320 (Contact With Jurors) that "(A) A member connected with a case shall not communicate directly or indirectly with anyone the member knows to be a member of the venire from which the jury will be selected for trial of that case. (B) During trial a member connected with the case shall not communicate directly or indirectly with any juror."

Now, enter the relatively new world of social media. Everyone knows that the addictive nature of e-gadgets and the miracle of the internet puts people online all the time posting biographical information and often mundane information about their daily activities. When the daily activity is their experience sitting in a courtroom, "wired" jurors create fits of hair-pulling exasperation for judges who, despite repeated admonitions during trial (as required by Penal Code 1122(b)) not to do so, still wind up with jury misconduct motions for new trials based on jurors communicating on-line about the case.

2. Counsel's Obligation to Research Jurors Online.

Yes, you read the heading correctly. Given the frequency of juror online misconduct, it is not only a good idea to check prospective and selected jurors activity on the internet and particularly social media, but as the NY City Bar Opinion puts it, we may have an obligation to do such research:

> "Just as the internet and social media appear to facilitate juror misconduct, the same tools have expanded an attorney's ability to conduct research on potential and sitting jurors, and clients now often expect that attorneys will conduct such research. Indeed, standards of competence and diligence may require doing everything reasonably possible to learn about the jurors who will sit in judgment on a case."

The Opinion quotes a published Missouri case where the court chastised the lawyers for not conducting online research on potential jurors so that they could have brought to the court's attention during voir dire that a juror lied about her prior litigation history with similar cases. The attorneys found out about the mendacity only after the adverse verdict to their client when they researched on-line public data. The trial court complained that it had to grant a new trial based on the juror's nondisclosure, but admonished: "in light of advances in technology allowing greater access to information that can inform a trial court about the past litigation history of venire members, it is appropriate to place a greater burden on the parties to bring such matters to the court's attention at an earlier stage." (Johnson v. McCullough, 306 S.W.3d 551, 558-59 (Mo. 2010). Indeed, "litigants should endeavor to prevent retrials by completing an early investigation." (Id. at 559.)

Further supportive of the duty of counsel to conduct online jury research during voir dire or during the trial, the Opinion cites another case where a New Jersey court found that a trial judge "acted unreasonably" by preventing counsel from using his laptop to conduct internet research of potential jurors IN COURT DURING VOIR DIRE! (Carino v. Muenzen, A-5491-08T1, 2010 N.J. Super. Unpub. LEXIS 2154, at *27 (N.J. Sup. Ct. App. Div. Aug. 30, 2010).) Obviously, trial attorneys would not have time to conduct computer research while in the midst of voir dire, but an assistant surely could.

The New York County Lawyers Association published Formal Opinion 743 stating that a lawyer may conduct juror research during voir dire and trial by visiting Twitter, Facebook and other similar social networking sites. It is "proper and ethical under [New York rules] for a lawyer to undertake a pretrial search of a prospective juror's social networking site, provided there is no contact or communication with the prospective juror and the lawyer does not seek to 'friend' jurors, subscribe to their Twitter accounts, send jurors tweets or otherwise contact them."

It should be noted that all these opinions and rules, including California's, state that if counsel does find misconduct by the juror, it must promptly reported to the court. Rule 5-320 requires: "(G) A member shall reveal promptly to the court improper conduct by a person who is either a member of a venire or a juror, or by another toward a person who is either a member of a venire or a juror or a member of his or her family, of which the member has knowledge."

In other words, attorneys cannot discover juror misconduct and then sit on it for tactical advantage while the trial goes forward confident of holding a trump card to nullify an adverse verdict post-trial.

3. How to Do Online Juror Research Without Running Afoul of #1 *Supra.*

Let's first establish the freezone of research where there should be no ethical problems. If one goes on the internet and looks at areas open to the public to inspect what comes up about a juror, there is no issue of an inappropriate communication with that juror. This is the equivalent of reading a news article on the juror or watching his or her conduct in public. It's plain view. Thus, "googling" a juror name and looking at the resulting "hits" should pose no problem. So long as the attorney (or investigator) is not attempting a communication, all is well. Of course, it goes without saying that any form of deceit to achieve a communication is forbidden (but I said it anyway).

But what if one merely views the person's social media site like Facebook? Just looking should not pose a problem, but if one goes further, such as by making a "friend" request of a sitting juror, that is clearly a prohibited ex parte communication. As the NY City Bar Opinion states, for a juror "to learn of the attorney's viewing or attempted viewing of the juror's pages, posts, or comments, that would constitute a prohibited communication if the attorney was aware that her actions would cause the juror to receive such message or notification." *See also* San Diego County Bar Assoc. Opn. 2011-2. The New York City Bar Opinion further states that it <u>may</u> even be unethical to make such a prohibited communication "even if inadvertent or unintended."

What does that mean? It means that if an attorney looks at juror information on a social media outlet like Facebook, Twitter or Linkedin, the site may be configured so that the juror receives information about any and all visitors to their site without the visitor even knowing this is happening. Thus, the attorney who looks at the Facebook page has no knowledge that this simple viewing of an "open" site results in a communication.

To avoid such unanticipated communications, the Opinion states: "Because of the differences from service to service and the high rate of change, the Committee believes that it is an attorney's duty to research and understand the properties of the service or website she wishes to use for jury research in order to avoid inadvertent communications."

This would require the attorney to understand the functionality of the social media site before embarking on a mere "look only" exploration. That is no easy task. We know that commercial enterprises look to see who is using the internet to shop at their store. They know if you have visited. How do we know this is so? Because shortly after your search you soon see on your internet pages advertisements for the very type of product which you searched in days previous. Your viewing sent a message of your interest with contact information which the web vendor took note of and then responded with targeted advertising. As Wikipedia says of the cookies that allow this: "Advertising companies

use third-party cookies to track a user across multiple sites. In particular, an advertising company can track a user across all pages where it has placed advertising images or web bugs. Knowledge of the pages visited by a user allows the advertising company to target advertisements to the user's presumed preferences."

Social media sites can do the same thing. For example, MyLife.com is a social network service that claims to help members find and keep in touch with others. You may have never heard of it but according to eBiz, it is the 13th largest social network in the U.S. with 5.4 million monthly visits. The site states that it will reveal to you the names of the persons who have performed searches looking for you. See Endnote.

The technology is there to communicate the fact that you visited a juror's media site. But it does not appear that, at the moment, Facebook tells a person who has visited their site. If you have a Facebook account you know you are not getting that information....for now. But it may be coming. My own website provides detailed statistical information on the number of visits each month without identifying the visitors. But adding that information does not seem difficult. Sites like Facebook have that ability (see Endnote) and change their functionality all the time. At one point, it gave everyone on Facebook a new email address (___@facebook.com) without asking if you wanted it. Also, in 2010, Facebook dramatically changed privacy settings on Facebook user accounts to greatly enlarge the amount of "public" information on the user's site even though the user did not intend to expose that information. The changes were announced after they took effect. In the wake of the uproar that followed, Facebook changed the rules to allow users to control their privacy settings. Bottom line: major social media sites change their functionality all the time.

4. California Rules and Potential Application

California Rule 5-320(E) states: "A member shall not directly or indirectly conduct an out of court investigation of a person who is either a member of a venire or a juror in a manner likely to influence the state of mind of such person in connection with present or future jury service." Implicit in this rule is that investigations of jurors during trial is permitted. Subsections (A) and (B) prohibits ex parte communications with venire or jury persons so this rule is aimed at investigations that might otherwise impact on a juror even without a direct communication. This appears to address, albeit unintentionally, the issue posed in the New York City Opinion where no direct and intended communication takes place, but one occurs because of the functionality of the juror's social media site. If a juror learns that counsel is looking at his or her site, is that a communication or investigation that is likely to influence their state of mind on the case? I would say "yes," and most likely that influence is going to be seen by the juror as an invasion of privacy or at least an unwanted intrusion by the attorney during the trial.

Add to these concerns section (F) of Rule 5-320 which states that the prohibitions stated in the rules apply not just to jurors but to the juror's family members: "All restrictions imposed by this rule also apply to communications with, or investigations of, members of the family of a person who is either a member of a venire or a juror." Also, the rule in subsection (I) defines the term "juror" to mean "any empanelled, discharged, or excused juror." (The expansiveness of this definition has obvious contradictions: can't an attorney communicate with an excused juror after the trial concludes?")

This new world creates problems. If we have a duty to investigate prospective and actual jurors for misconduct (and gather informative biographical information of interest), how can this be done if a generalized google search sends a message to the juror informing that we are looking at them? As of now, this is not a problem on the major media sites, but, as the New York City Bar Opinion suggests, we need to maintain our awareness of what the sites are communicating to others.

ENDNOTE: Here are what three media sites say about their policies on collecting information about who you are searching for and, as with Classmates and MyLife, passing that information on to the person being searched.

Facebook.com: "We receive data about you whenever you interact with Facebook, such as when you look at another person's timeline, send or receive a message, search for a friend or a Page, click on, view or otherwise interact with things, use a Facebook mobile app, or purchase Facebook Credits or make other purchases through Facebook."

Classmates.com: "Every time that you visit another member's profile, your name and the date of your visit will be viewable by that member as someone who visited that member's profile unless you opt out of having your name automatically left on other members' profiles, which you can do by accessing the "Account" section on the Website and changing your preferences. If you opt out of automatically having your name left on other members' profiles, you will still have the ability to leave your name on specific members' profiles on an individual basis."

MyLife.com: "Searches. When you search for another person while logged into MyLife, your search may be shared via our Who's Searching for You feature. With this feature, another member may be notified if you have searched for someone with a name matching theirs. Other members also may be notified if you view their profile while logged into MyLife.com."

Have Laptop, Don't Travel

By
Chuck Sevilla

One area close to home (and office) where privacy rights have taken a distinct back seat to government power is that of the computer. If you travel outside the United States with a laptop (or an equivalent device like a PDA, I-pad, Smart phone), the government can take it upon your re-entry for no reason whatsoever except curiosity to see what is inside.

As a result of this, many corporations have strict rules in place to forbid employees from traveling abroad with any company data on their laptops. For those of us who have attorney-client information on our laptops, the necessity for precaution would seem every bit as great. But let's talk about the cases first.

In U.S. v. Arnold, 523 F.3d 941, 942 (9th Cir. 2008), the question was posed: "We must decide whether customs officers at Los Angeles International Airport may examine the electronic contents of a passenger's laptop computer without reasonable suspicion." Answer: yes.

Michael Arnold arrived at LAX after a long flight from the Philippines. After retrieving his luggage, he went through customs and was selected for questioning. Arnold stated that he had been on vacation visiting friends in the Philippines. His luggage was inspected. He had with him his laptop computer, a separate hard drive, a USB drive, and six CDs. He was told to turn on his computer. The agents opened files on the laptop and viewed a photo showing two nude women. That led to hours of detention and questioning. Upon further inspection, the computer revealed more images depicting child pornography. The computer was seized as were the storage devices. Arnold was criminally charged and moved to suppress the laptop search for lack of a reasonable suspicion. The trial court granted his motion.

The Ninth Circuit reversed the suppression ruling. It held: "Courts have long held that searches of closed containers and their contents can be conducted at the border without particularized suspicion under the Fourth Amendment." Id., at 944. The only possible exceptions to the rule are when the search is completely destructive of the item, or where, as with a search of a person's "alimentary canal," human dignity is transgressed. Neither issue, said the court, is involved in the case of turning on a laptop and inspecting its contents. *Accord* U.S. v. Ickes, 393 F.3d 501, 506-08 (4th Cir. 2005).

An exception to the above "border search" rationale for computer searches without cause is U.S. v. Cotterman, 709 F.3d 952 (9th Cir. en banc 2013). While returning home from a trip to Mexico, Cotterman's laptop computer was confiscated by border agents after an initial border inspection revealed his status as a sex offender. A search of his revealed a laptop with password-protected files. Unable to open the files at the border, the laptop was sent to an INS office 170 miles away for a full forensic examination. The district court granted Wesley's motion to suppress the evidence found on his laptop, finding that the border agents lacked reasonable suspicion to conduct the "extended border search." The government filed an interlocutory appeal. The Ninth Circuit rejected the application of the "extended border search" doctrine in this case simply because the forensic examination was conducted at a location so far away from the border. It found the intrusiveness of a full forensic examination of a laptop computer, regardless of the location, does require a showing of reasonable suspicion because substantial privacy interests are implicated. The Court held that reasonable suspicion was satisfied in this case under a totality of the circumstances.

California has weighed in on the issue in like manner. "Indeed, the human race has not yet, at least, become so robotic that opening a computer is similar to a strip search or body cavity search. Of course viewing confidential computer files implicates dignity and privacy interests. But no more so than opening a locked briefcase, which may contain writings describing the owner's intimate thoughts or photographs depicting child pornography. A computer is entitled to no more protection than any other container. The suspicionless border search of Endacott's computer was valid." People v. Endacott, 164 Cal. App. 4th 1346, 1350 (2008).

It's no better when your cruise ship docks and you disembark to clear customs. However, a recent case has held that the border search doctrine will not apply to search a cabin on a cruise ship that has docked without reasonable suspicion. This is because "[t]he cruise ship cabin is both living quarters and located at the national border." U.S. v. Whitted, 541 F.3d 480, 488 (3d Cir. 2008). But if you disembark and go through Customs, border search rules apply and no suspicion is needed to search your computer.

But does the border search doctrine allow the search of privileged documents inside the computer? In United States v. Seljan, 547 F.3d 993, 1003 (9th Cir. En banc 2008), the majority held that letters enclosed in FedEx packages with foreign destinations are subject to the border search rule allowing free examination even though they would be protected if the recipients lived in the United States.

However, we don't want to risk having to litigate the privilege issue in court in order to retrieve sensitive material on the computer involving clients? What would your

client think about that? Do we have an ethical duty to insure that such material does not come within the purview of the government? I would think so.

So what options does that leave for traveling lawyers with laptops? Some suggestions: You could strip the computer of all sensitive material and leave that material in the office. Unless the computer hard drive is "wiped" clean with an appropriate program, just using the conventional "delete" function will not remove the material from the computer and it will remain accessible.

What about encrypting privileged files? That would remove a "plain view" doctrine theory of discovery and also make a further search of those files much more intrusive. See *In re Grand Jury Subpoena,* 670 F.3d 133 (11th Cir. 2013) (grand jury witness may take Fifth Amendment to questions seeking the password key to open his encrypted seized computer). Whether it would raise the level of required suspicion from nothing to a "reasonable suspicion" is doubtful. Looming behind all these border search cases is the fear of terrorists bringing in plans for our destruction. Thus, encryption may only raise insure a more intensive search.

Perhaps the soundest alternative is to travel with a clean laptop and then use a remote access software such as GoToMyPC or LogMeIn when arriving at the foreign destination. These programs allow remote access from your laptop through the internet back to your office, allowing you to work on the office computer and not having to have any files in the laptop.

One final note about computer searches unrelated to the border search area. Two California cases have held that computers may be seized in home searches pursuant to warrant even if not mentioned in the warrant. They can be seized to establish "dominion and control" of the premises. People v. Varghese, 162 Cal. App. 4th 1084, 1100 (2008); People v. Balint, 138 Cal.App.4th 200, 205 (2006). These courts held that the "computer is the functional equivalent of a filing cabinet and a reasonable place to seek information concerning the dominion and control of the place searched." Varghese, *supra* at 1101. In the latter case, the court allowed the "dominion and control" of the residence theory to justify the computer seizure even though the laptop was found in a car outside the house.

Clearly, the contents of your computer are getting tougher to protect.[10]

---

[10] Note that turning a laptop in for repair to a computer tech means the loss for Fourth Amendment protection. *See* U.S. v. Tosti, 733 F.3d 816, 822-823 (9th Cir. 2013). Also, such technicians are now mandated reporters in California.

What's Up With Cell Phone Searches? Riley v. CA is What!

In People v. Diaz (2011) 51 Cal.4th 84, the California Supreme Court held 5-2 that the Fourth Amendment's search-incident-to-arrest doctrine permits the police to search a cell phone whenever the phone is "immediately associated with [the arrestee's] person" at the time of the arrest. **The Court was overruled by Riley v. California,** 134 S. Ct. 2473, 189 L.Ed.2d 430 (2014), on June 25, 2014: "We therefore decline to extend Robinson to searches of data on cell phones, and hold instead that officers must generally secure a warrant before conducting such a search."

Interestingly, Mr. Diaz had filed a petition for a writ of certiorari to the U.S. Supreme Court. Shortly thereafter, the California Legislature passed a bill requiring the police to obtain a search warrant before searching the contents of any "'portable electronic devices,' including cellular telephones." (Senate Bill 914 (2011)). The State brought this bill to the Supreme Court's attention and urged the Court to deny review which it did. 132 S. Ct. 94 (2011). A week later, Governor Brown vetoed the bill stating that the "courts are better suited to resolve the complex and case-specific issues relating to constitutional search-and- seizures protections." (!) http://www.leginfo.ca.gov/pub/11-12/bill /sen/sb_0901-0950/sb_914_vt_20111009.html.

Other courts agree with requring warranted searches of cell phones. Smallwood v. State (Fla. 2013) 113 So. 3d 724, 740 ("while law enforcement officers properly separated and assumed possession of a cell phone from Smallwood's person during the search incident to arrest, a warrant was required before the information, data, and content of the cell phone could be accessed and searched by law enforcement"); State v. Smith (Ohio 2009) 920 N.E.2d 949, 955 ["because a person has a high expectation of privacy in a cell phone's contents," police, after seizing a cell phone from an arrestee's person, "must … obtain a warrant before intruding into the phone's contents"); *see also* U.S. v. Wurie (1st Cir. 2013) 724 F.3d 255 (denial of en banc) and 2013 U.S. App. LEXIS 9937, cert pending (search-incident-to-arrest exception did not authorize the warrantless search of data on the cell phone seized from defendant's person). Wurie is a companion case with Riley

Recent case of note: U.S. v. Lopez-Cruz (9th Cir. 2013) 730 F.3d 803, holding a peace officer exceeds the scope of consent to "look in" or "search" a cellular phone when he answers incoming calls.

Metadata and You

By
Chuck Sevilla

In August 2007, the California State Bar issued a Formal Ethics Opinion No. 2007-174. *See* http://calbar.ca.gov/calbar/pdfs/ethics/2007-174.pdf. It addresses questions about counsel's duty to release e-versions of matter collected during the representation of a client after employment ends.

The Opinion answers the following questions: Is an attorney ethically obligated, upon termination of employment, promptly to release to a client, at the client's request, (1) an electronic version of e-mail correspondence? **Yes.** (2) an electronic version of the pleadings? **Yes.** (3) an electronic version of discovery requests and responses. **Yes.** (4) an electronic deposition and exhibit database? **Yes.** (5) an electronic version of transactional documents? **Yes.** All of these questions are answered by Rule of Professional Conduct 3-700(D), the duty to promptly turn over to the client "all papers and property." This Opinion simply clarifies that the latter phrase includes electronic versions of "paper and property." There is nothing particularly startling about these conclusions.

I might add another issue resolved by the Opinion. Say you are loyal to Word Perfect and don't use Word. The client wants all your electronic files in his/her case sent in Word format. Do you have to convert them? **No.** Your obligation is only to release the items you have, not to create or convert them.

The end of the Opinion discusses stripping of metadata from the e-documents you release. The Opinion advises that before releasing any of the above data to the client, counsel must adhere to the Bus. & Professions Code requirement protecting client confidences. That means stripping all metadata reflecting confidential information belonging to *other* clients.

Never heard of metadata? It is stored on every one of your word processed files? According to Wikipedia, metadata is a generic term for data used to facilitate the understanding, use and management of data. For example, on your IPod, album names, song titles and album art are embedded in the music files and are used to generate the artist and song listings.

Metadata has proved helpful in other ways. The author of the Melissa virus in 1999 was caught due to metadata that identified the computer he used to create the

original infected document. Nice.

On word processed documents (MS Word and WordPerfect), your files include metadata. This is data you don't see when you print out your document. As with the IPod song, it is embedded in the document and may include the original author's name, the creation date of the document, and the amount of time spent editing it. It can be seen simply by clicking "File," and then "Properties" on either Word or WordPerfect.

Now, here's the rub: unintentional disclosure of metadata can raise malpractice concerns by revealing the name of the person who last edited the file, how many times the file has been printed, how many revisions have been made on the file, the deleted text (saved in case of an undelete command), document comments from editors, and the suggested edits. On WordPerfect X3, you can add all these and many more metadata attributes you wish to see. Once inside the Properties file go to "setup" and add anything and everything you want.

As you can imagine, inadvertent inclusion of this material in distributed files may sometimes prove embarrassing if not legally undesirable.

Stripping metadata. Fortunately, there are easy ways to strip a file of metadata. In WordPerfect X3, just go to "File" and look down the list for "Save Without Metadata." Inside that option, there are many boxes to check as to the material you want stripped. Then save the file which creates a new file with an "mtd" file extension. This function does not change or harm the original document. Check the meta file now through "Properties" and see if everything you want extracted is out. (I could not find this function in WordPerfect editions prior to X3, so this may be a reason to upgrade.)

There are also freeware metadata analyzers on the internet. *See, e.g.*, http://www.bestfreewaredownload.com/download/t-free-metadata-analyzer-freeware-asesznca.html.

You can also effect changes in the meta file through "Properties" in your word processing document. Thus, if you want to leave in data, you can dictate what data that will be. By the way, converting a file from Word or Word Perfect to "pdf" does not necessarily eliminate metadata. So strip your file before converting to pdf.

There are many horror stories reported about the inclusion of metadata. Perhaps the most notorious example involved the New England Journal of Medicine. That respected journal reported that Merck & Co. deleted information from a document submitted to it for publication. The deleted material connected Vioxx to an increased risk

of heart disease. The "deleted" information was found in the metadata embedded in the document.

Other examples:

> By this time, almost everyone has heard metadata horror stories, including court briefs including such recoverable draft comments as "Judge XXXX isn't very bright, but even a fool wouldn't buy this argument." Or how about the partner who had his associate draft a very important contract for a client and then billed the entire matter at partner rates? He's up on disciplinary charges, hoisted on his own petard by the document's metadata." Sharon D. Nelson, Esq. and John W. Simek, "Cool Technology for Hot Lawyers," p. 3, The Vermont Bar Journal (Summer 2007).

(Law firms that circulate drafts of pleading for comments, take note.)

Let's apply the above example in our work. Say your opponent in a case sends you an e-pleading he/she just filed with the court. You check the metadata and note some interesting deletions – such as the deletion of a citation to the controlling case in your favor. Intentionally misleading the court by not citing controlling law is unethical. When brought to the attention of the court, it will destroy the credibility of the other side. (But read on, this gets more complicated.)

The potential problems with metadata are obvious. Here's another one. Is it ethical for an attorney *to even look at* embedded metadata sent by the opponent? That may seem like a silly question. If an attorney sends out a letter, report or pleading in e-form, why can't you look at the metadata that comes with it? I say, no problem. Much of the metadata is of no real import.

But what if in looking you come across confidential material such as work product (*e.g.*, edits or comments left in the documents)? Intuitively, one might say, "Eureka! I have found it!" and exploit the material for all it's worth. But consider this:

In Rico v. Mitsubishi (2007) 42 Cal. 4th 807, the Supreme Court dealt with an issue of the inadvertent disclosure of work product to one's adversary. The context was a motion to disqualify counsel in a civil case because the latter innocently obtained written work product of the other side and then used it. The rule announced in the case was this: an attorney who receives a privileged document of an adversary through inadvertence may not read it any more closely than is necessary to ascertain it is privileged. Once that threshold is reached, the attorney must notify the other side and try to resolve the

situation. This rule applies even if the documents are not marked privileged and the other side was negligent in divulging the material. This holding may control the metadata issue. The Court considered the practical problems of allowing attorneys to exploit inadvertently revealed confidences:

> the practical problem of inadvertent disclosure in the context of today's reality [is] that document production may involve massive numbers of documents. A contrary holding could severely disrupt the discovery process. As amicus curiae the Product Liability Advisory Council, Inc., argues, "Even apart from the inadvertent disclosure problem, the party responding to a request for mass production must engage in a laborious, time consuming process. If the document producer is confronted with the additional prospect that any privileged documents inadvertently produced will become fair game for the opposition, the minute screening and re-screening that inevitably would follow not only would add enormously to that burden but would slow the pace of discovery to a degree sharply at odds with the general goal of expediting litigation." Id. at 818.

Robert D. Brownstone's article, "Metadata: To Scrub or Not to Scrub," pp. 9-10, California Bar Journal (Feb. 2008), notes the States are all over the map on how to deal with this ethical issue, but he cites Rico as California law on this topic. While Rico relates to hard copy inadvertent disclosure, there is no reason in logic or practice it would be limited to paper and excluded e-file disclosure.

For now, the safest step is to strip metadata from all files leaving your computer no matter to whom they are being sent. That insures compliance with the Ethics Opinion and safeguards against inadvertent disclosures that could both prove embarrassing and bring about adverse legal consequences for clients.

Citizens Recording Public Police Conduct

By: Chuck Sevilla

Your clients are walking down the street and see several members of the local constabulary using billy clubs to firmly remind several handcuffed and street prone citizens of their duties to remain quietly unconscious. The alert officers detect that they are being video recorded by your clients through the use of their excellent smart phone cameras. They loudly inform the clients to cease and desist their filming. The clients do not reply and just keep the cameras rolling while several officers continue administering blows to the downed and helpless citizenry. One cop approaches the filmers and grabs at their phones. They say, "fuck off and leave my stuff alone!" The officer promptly orders their arrest for assault, resisting arrest and obstruction of justice. Other officers come to the aid of the arresting cop and perfect their arrests and cuffing. Then the newly arrested citizens receive the same lumps and bumps as the subjects of their abruptly shortened documentary on police abuse. According to subsequent police reports, their phones are accidently destroyed in the melee.

You represent the filming clients. In their defense, you want to introduce their videos which miraculously survived the encounters only because several of them swiftly sent their recordings to their home email address prior to confiscation and destruction. When you seek admission, the prosecution argues that the filming of the police encounter was a violation of the state wiretapping laws

This is not a made up story. "A number of citizens throughout the country say they have been charged with a crime (often obstruction) while recording police on the job." One Californian was arrested this past month in Hawthorn while filming police on a public street. The obstruction charges were later dropped. See ABAJournal.com, Martha Neil, "Supreme Court Gives Nod to Citizens Who Record Police, Amidst Reports of Multiple Arrests," Nov. 26, 2012.

The purpose of this Flash is to alert you to a Seventh Circuit case, ACLU of Illinois v. Anita Alvarez, 679 F.3d. 583 (7th Cir. 2012) cert. denied sub nom. Alvarez v. ACLU, 133 S. Ct. 651, 184 L. Ed. 2d 459 (2012). In that case, the ACLU planned a "police accountability program," which included a program to openly make audiovisual recordings of police officers performing their duties in public places while talking at a volume audible to bystanders. Worried that starting this program would result in arrests of their videographers under the Illinois eavesdropping statute, the ACLU filed a pre-enforcement action asking for declaratory and injunctive relief barring the enforcement of the statute as applied to their audio and video recordings. The district

court judge ruled that the First Amendment did not protect a right to audio record the police even in public settings.

On appeal, the ACLU prevailed. The State argued that its eavesdropping statute precluded such recordings. The court of appeal disagreed. The court held that protecting conversational privacy was not implicated when police officers are performing their duties in public places and engaging in public communications audible to persons who witness the events. The eavesdropping statute, at least as applied, would restrict far more speech than necessary to protect legitimate privacy interests. "Illinois has criminalized the nonconsensual recording of most any oral communication, including recordings of public officials doing the public's business in public and regardless of whether the recording is open or surreptitious." (ACLU v. Alvarez, supra at 586.) "As best we can tell, the Illinois statute is the broadest of its kind; no other wiretapping or eavesdropping statute prohibits the open recording of police officers lacking any expectation of privacy."
(Id. at 595.)

Judge Posner dissents. First, he notes that the "statutes of several states are so open-ended that they could easily be found invalid under the approach taken in the majority opinion." He cites as a prime example Cal. Penal Code § 632(c). He says our statute is "illustrative. It states that 'the term "confidential communication" includes any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering or in any legislative, judicial, executive or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded.' The words are clear, the meaning is clear, but the application is unclear. Should a conversation in a public place, but intended to be private, be thought a 'communication that any party desires to be confined to the parties'? It is both intended to be private and remote from a communication made in a 'public gathering,' a term that from its placement connotes a public meeting of some sort. But what of the exclusion of private communications that the parties 'may reasonably expect... may be overheard or recorded'? That fogs the issue of which private communications are protected. To read the statute literally would exclude all private communications, for any private communication can be overheard and recorded, even if it is a conversation in a closed room." (ACLU v. Alvarez, supra at 609.)

Judge Posner wonders about the application of the majority rule to the private person being filmed. Thus, what if the person talking with a police officer is a suspect, an informant, a bystander whom the police are shooing away from the scene of a crime or an

accident, an injured person seeking help, a crime victim seeking police intervention, someone simply asking for directions, or someone arguing over a parking ticket or reporting a traffic accident? "In many of these encounters the person conversing with the police officer may be very averse to the conversation's being broadcast on the evening news or blogged throughout the world. In some instances such publicity would violate the tort right of privacy."
(Id. at 611.)

Those are legitimate issues that will play out in the future. However, the thrust of the opinion on the facts presented is a good one: police have no right to privacy in carrying out official duties in public and can be filmed carrying out their actions. Recall that cases like the one involving the beating of Rodney King came about only because a bystander videotaped it. The pervasive existence of phone cameras may alone be a significant deterrent to police misconduct. If not, resulting citizen videos will bring to justice those who violate their oaths to uphold the law.

P.S. If you are concerned about the client telling the officers to fuck off, see People v. Callahan (1985) 168 Cal.App.3d 631 (held free speech absolves a defendant of his conviction for uttering offensive words in public which were inherently likely to provoke an immediate violent reaction - he called the cop a "fucking asshole," among other profanities.) As the court stated, the citizen was trying to get the attention of the officer (he certainly did-he got arrested). But the words, said the court, are but a modern update: "Fifty years ago the words 'damn' and 'hell' were as shocking to the sensibilities of some people as the Callahan epithet is to others today. The first word in Callahan's epithet has many meanings. When speaking about coitus, not everyone can be an F. E. Smith (later Earl of Birkenhead) who, in his speech in 1920 in the House of Commons on the Matrimonial Causes Act, referred to 'that bond by which nature in its ingenious telepathy has contrived to secure and render agreeable the perpetuation of the species.'"

Using Unallocated Computer Space Images to Convict

By Chuck Sevilla

Did you know there are images on your computer you don't know about and have no way of seeing? The following discussion may seem technical, but it's as simple as it is important: images on computers which the owner does not even know about can be damning, particularly when the images constitute child pornography.

This is the story of images in the unallocated space of your computer. It's what I've learned in a case I'm now handling. You can't see files in unallocated space without special software. However, with that special software, law enforcement routinely examines for files and images in the "unallocated space" of the computer's hard disk.

What's unallocated space you ask? Allocated space is the hard drive space where files exist. You see them. They can be program files or files you created, named and saved like a brief, email, or photo. Unallocated space is that area of the hard drive where there are no active files and no references to them. The operating system is not using them because they are "deleted." But they really aren't. Think of allocated space as the world you see, live and work in, populated by files and images you created, downloaded and saved. Think of unallocated computer space as outer space, the apparent enormous black void but which actually contains file castoffs waiting to be annihilated by the great operating system in the sky, or discovered by law enforcement.

Now back to how deleting files doesn't really delete them. When images or text files are "deleted," they don't disappear but rather go into the unseen world of unallocated space. The only way they can be erased is by being overwritten (as with a file download or new operating software installation) or deleted with special software. Note: just because you download a new operating system (OS) does not mean everything on the hard drive is overwritten. If the new OS takes up five percent of your hard drive, that's the space being overwritten.

When images are found in the unallocated space, in many cases, even an expert cannot tell if they were ever viewed. The expert may not even be able to tell when they were created or where the files were originally stored. An expert cannot even tell if the computer owner ever opened or had knowledge of files in unallocated space.

All the expert can say is that the images were at one time on the hard drive and were deleted either by a user action or the operating system's normal processes.
How does a file get deleted from allocated space by the operating system? A typical

scenario is for images to arrive in the computer's temporary internet storage file area when the user is browsing the Internet. You can find and see these images. Images on an internet web page are automatically placed in temporary internet storage area by the web browser for faster browsing (also know as cashing). The user doesn't see the actual file being downloaded. Later, to save space, the temporary internet storage folder will be automatically cleansed by the operating system and the files "deleted;" *i.e.*, relegated to the unallocated space. There they sit unseen, unknown and undisturbed until either being overwritten or deleted by someone who has access to them.

(It might be noted that with the universe of hard drive storage being so large, files in unallocated space may be spared for a long time from being randomly overwritten.)

In the real world, if someone browsed a website that advertised adult pornography images, the latter would go to the temporary internet file folder. Through normal use, that file folder would, in time, be automatically deleted by the operating system, the web browser, or the user himself, and those images would go to unallocated file space.

In the case I'm handling, an expert testified that adult "pornographic websites, many known as portals ... contain thumbnail images like this [child porn thumbnail images] as kind of previews to what the website might offer.... the adult website that is the portal, is not a site that's really hosting any content themselves. They're just pointing to websites." Child pornography images are embedded on hundreds of adult sites. A visit to the site can result in unintentional downloads of webpage images. These go the temporary holding area on the computer and then ultimately are "deleted" and sent to unallocated space. Typically, these are small thumbnail size images.

Other means by which nasty thumbnail images could land in the computer's unallocated space (other than purposefully) in addition to web surfing, are through an e-mail, spam, or someone directly sending it to an e-mail address which someone on the computer used. Another way would be if someone plugged a thumb drive into the computer and transferred the images on to it. Also, if one bought a used computer, the images could have been on the hard drive. Or, usage by guests, relatives, or repair people could be the source of the images. Also, read about the case of a fellow whose computer was invaded by a Trojan Horse that populated his computer with child porn. See "Trojan Horse Found Responsible for Child Porn," by Munir Kotadia, August 1, 2003, at http://www.zdnet.com/trojan-horse-found-responsible-for-child-porn-3039115422/. See news articles at the end of this chapter.

Bottom line, there is no way to determine the derivation of images located in unallocated space.

What is the legal challenge to keep this evidence out? In my case, the defendant had nothing in his computer indicating an interest in any kind of pornography. That is, in checking stored files, the web browser search history, email, nothing was found. Further, the house had no magazines, CDs or DVDs containing pornography. Nevertheless, the judge let in two thumbnail images depicting young girls in suggestive poses from unallocated space as Evidence Code section 1108 propensity evidence to commit a child molestation.

Here's why that ruling was wrong. The judge said the defendant had the computer in his house, owned it, and thus had access to it. But that's not good enough. People v. Falsetta (1999) 21 Cal.4th 903, 917, states that a trial judge must consider when evaluating propensity evidence "the degree of certainty of its commission." There is nothing close to certainty when dealing with images in unallocated space especially from a computer that is open to use by others. The only California case that comes close to saying this is Tecklenburg v. Appellate Division (2009)169 Cal.App.4th 1402 which stated: "Defendant was one of the users of the home computer. He was the registered owner of that computer. This, of course, *would not be sufficient alone* to show he was the person who had entered the word searches or Web site addresses or accessed the Internet images and graphics found on the home computer." (Id. at 1413.)[11]

In other words, access and ownership are insufficient to tie such hidden images to the defendant. Other cases agree. (*See* U.S. v. Flyer (9th Cir. 2011) 633 F.3d 911 [conviction reversed for insufficiency of evidence that Flyer knowingly possessed child pornographic images found in unallocated space on his computer*;* U.S. v. Moreland (5th Cir. 2011) 665 F.3d 137, 154 [court reversed a child pornography conviction where images were found only in unallocated space because "the evidence is insufficient where the defendant exclusively possessed that computer, without additional evidence of the defendant's knowledge and dominion or control of the images"]; Oregon v. Ritchie (2011) 349 Ore. 572 [defendant was charged with controlling photographs of sexually explicit conduct involving children; some were recovered from unallocated space on a desktop computer's hard drive which were derived from browsing the internet; the evidence was

---

[11] *See* People v. Mahoney (2013) 220 Cal. App. 4th 781, where the court upheld possession of child porn pictures in the defendant's temporary internet files and unallocated space. The court distinguished U.S. v. Kuchinski (9th Cir. 1990) 469 F.3d 853 because this was a sophisticated computer use who, according to the prosecution's expert, actively searched the Internet for child pornography and erotica and opened such sites. Therefor, there was evidence the jury could rely on to find knowledge of the contents of the temporary internet files.

held insufficient to support a finding of possession or control].)

These cases are helpful not only to keep out images from unallocated space when they are offered as propensity evidence, but also as grounds to argue insufficiency of evidence where they are the evidence for a charge of pornography possession.

Caution: Finding Porn on Computers: Quite Possible for Them to Be Planted
Trojan Horse Found Responsible for Child Porn

By Munir Kotadia | August 1, 2003 -- 14:40 GMT (07:40 PDT) **ZDNET news item**
Summary: A man has been cleared of child porn charges, after investigators found that an Internet attacker was responsible for the presence of illicit images on his PC

A man accused of storing child pornography on his computer has been cleared after it emerged that his computer had been infected by a Trojan horse, which was responsible for transferring the images onto his PC.

Julian Green, 45, was taken into custody last October after police with a search warrant raided his house. He then spent a night in a police cell, nine days in Exeter prison and three months in a bail hostel. During this time, his ex-wife won custody of his seven year old daughter and possession of his house.

This is thought to be the second case in the UK where a "Trojan defence" has been used to clear someone of such an accusation. In April, a man from Reading was found not guilty of the crime after experts testified that a Trojan could have been responsible for the presence of 14 child porn images on his PC.

Trojan horses can be used to install a back door on a PC, allowing an attacker to freely access the computer. Using the back door, a malicious user can send pictures or other files to the victim's computer or use the infected machine to access illegal Web sites, while hiding the intruder's identity. Infected machines can be used for storing files without the knowledge of the computer's owner.

Kevin Hogan, senior manager at Symantec Security Response, told ZDNet UK that he has known Trojans to pretend to be a game, picture and even a Windows folder. "It is technically possible for a Trojan to set up someone's computer as a proxy machine. So you see a folder on your desktop, double click it and it executes."

According to Hogan, a Trojan back door can usually be dealt with by using an up-to-date antivirus software or a personal firewall.

Green told The Evening Standard that the experience wrecked his life because he was treated like a depraved sex fiend. "I had never been in trouble before. In cases like this it is not innocent until proved guilty, but the other way around," he said.

Green is reportedly planning on suing the police for compensation.
http://www.zdnet.com/trojan-horse-found-responsible-for-child-porn-3039115422/

United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012)

Getting the software via discovery: this case has application in many discovery areas such as DUI cases where the defense seeks the software code used by the breathalyser. It also is a lesson in why not to use peer-to-peer software (because it opens the door for anyone, including law enforcement, to look into your computer files). Clients involved in sharing child pornography through such software are marks for arrest and the horrendous federal sentences for such crimes.

FBI agents using an "EP2P" program to search for child porn (an enhanced version of Limewire), downloaded images and found porn at an IP address associated with Budziak. A later search of his house revealed a computer with Limewire, and child porn videos. Budziak was convicted after trial of distribution of child porn.

He contended the evidence presented at trial was insufficient to convict him of distribution arguing that evidence of a deliberate, affirmative action of delivery is required to support a conviction for distribution. He argued that just storing child pornography in a shared folder accessible to other LimeWire users is insufficient because it is evidence of no more than passive possession. Rejected. "Following the First, Eighth, and Tenth Circuits, we hold that the evidence is sufficient to support a conviction for distribution under 18 U.S.C. § 2252(a)(2) when it shows that the defendant maintained child pornography in a shared folder, knew that doing so would allow others to download it, and another person actually downloaded it."

In United States v. Borowy 595 F.3d 1045 (9th Cir. 2010), the Circuit reiterated that no one has an expectation of privacy if one's computer is hooked up to peer-to-peer file sharing software. *Accord* U.S. v. Ganoe, 583 F.3d 1117 (9th Cir. 2008) (being on a file sharing program is an open invitation for all to "come on in" and there is no right of privacy violation if others do search one's computer.) Child porn prosecutions can produce horrendously long sentences. *E.g.*, U.S. v. Steiger, 318 F.3d 1039, 1043-1044 (11th Cir. 2003) (The Turkish hacker stated: "How did I get access to his PC? I used the well known Trojan horse named Subseven... I made it undetectable so av [anti-virus] softwares [sic] couldnt [sic] see it and bind it with a fake program;" this led to a search warrant, prosecution and a 235 month sentence for possession of child porn); U.S. v. Jarrett, 338 F.3d 339 (4th Cir. 2003) (same hacker held not a state agent despite trial court finding otherwise because hacker used same FBI agent as in Steiger who said "give us more" and promised no prosecution for his crimes. Similarly long sentence.)

Budziak is notable for this: the FBI hacked Limewire into "EP2P," used it to find the porn, then *refused to disclose the software at Budziak's trial* -- making it impossible

for him to challenge. The court held that in "cases where the defendant has demonstrated materiality, the district court should not merely defer to government assertions that discovery would be fruitless. While we have no reason to doubt the government's good faith in such matters, criminal defendants should not have to rely solely on the government's word that further discovery is unnecessary. This is especially so where, as here, a charge against the defendant is predicated largely on computer software functioning in the manner described by the government, and the government is the only party with access to that software. **Accordingly, we hold that it was an abuse of discretion for the district court to deny Budziak discovery on the EP2P program."**

AUTHENTICATION OF E-DOCS

Authentication: "(a) the introduction of evidence sufficient to sustain a finding that it is the writing that the proponent of the evidence claims it is or (b) the establishment of such facts by any other means provided by law." (CA Evid. Code, § 1400.)

Information and Pictures from the Internet–Beckley

The defendant's girlfriend testified that he wasn't in a gang nor was she. A picture was from the defendant's MySpace page was admitted showing her throwing a gang sign. The Court of Appeal finds error because no one could authenticate the digital picture, which is easy to tamper with. The prosecution also got into evidence an Internet page listing the membership of the Southside Compton Crips, to prove that the defendant was a gang member. The testifying police officer believed that the gang maintained the list. But there was nothing to authenticate the list as being accurate. (People v. Beckley (2010) 185 Cal.App.4th 509)

Internet Information–Valdez

Defendant had a password protected MySpace page where he posted pictures of himself throwing gang signs and comments about what a gang banger he was. The police gang expert relied on this to conclude the defendant was a member of the gang. The prosecution investigator testified he printed the web pages in May 2006, a year before the shootings in the case. He testified that although a person's MySpace pages are accessible to the public, these pages were password protected so only the creator of the pages or those who have access to the password could upload or manipulate its content. The appeals court holds that the foundation laid at trial by the expert satisfied authentication requirements. (People v. Valdez (2011) 201 Cal.App.4th 1429.)

Computer-generated Cell Phone Records

The prosecution got into evidence cell phone records consisting of "a computer printout of automatically generated and stored call data." The records were from a printout "where the printout is produced by human query for use at trial." Such records are deemed as business records once the Evidence Code section 1271 foundation is laid and where it is shown that "the underlying data is kept and maintained by a reliable computer program in the regular course of business." Here, the prosecution called a representative of Sprint to lay the foundation describing both how Sprint maintains such records and how the records were generated in response to a subpoena. Because the underlying data wasn't produced by human input but instead was automatically recorded by the computer system, this solidified the business record nature of the document. (People v. Zavala (2013) 216 Cal.App.4th 242.)

See In re K.B. (2015) 238 Cal.App.4th 989, where the court upheld the authentication of an Instagram photo on a cell phone belonging to the third party as evidence against the defendant.

A Word About Compilations.

In People v. Franzen (2012) 210 Cal.App.4th 1193, the trial court erred by admitting the evidence from a Web site under the "published compilation" exception to the hearsay rule. Here, “an aggregation of whatever information the Web site operators could find associating names with phone numbers” was complied using “Entersect.” The only fact attributed to the Entersect site was that the second of two phones used to arrange the drug sale was the defendant's. When the defendant was arrested she was in possession of this same phone. This Entersect evidence was allowed into evidence as a hearsay exception for "published compilations" set forth in Evidence Code section 1340. The appeals court held that the Entersect compilation was not "generally used and relied upon as accurate" in the course of the department's "business." It should not have been admitted; however, the error was harmless in this case. The following language from the opinion is noteworthy.

> Section 1340 was manifestly not intended to permit the introduction over a hearsay objection of "information that's out there." "Information" does not become "evidence" merely because someone finds it worth seeing. The Internet contains, or more accurately is connected to and thus capable of conveying, a large and growing part of all of the recordable information in existence. Some of this information is as reliable as any traditional source of information. But some of it would be almost universally considered not only unreliable but extravagantly untrue. If this technology provides the means to store and convey every truth any human has ever articulated, it also has the capability of "publishing" every misconception, error, delusion, or outright lie anyone has ever set down. The world of print has known its share of infamous frauds, libels, and fantasies packaged as fact, but at least the cost and difficulty of publication has had some tendency to inhibit the circulation of erroneous information. That inhibition has now all but disappeared. And while the absence of barriers to publication may promise a true "marketplace of ideas," it also means that the mere fact of publication cannot be relied upon to furnish any assurance of reliability.

(Id. at 1212.)

A Few Out of State Authentication Cases. Generally, authenticating paperless e-evidence may not be easy, but with some thought about it, it can be done. In Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 546 (D. Md. 2007), the court exhaustively explores

the issues involved in authentication of ESI (electronically stored information) and is well worth reading when attempting to authenticate text messages, emails, or web postings. See cases cited therein: U.S. v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (authentication of an e-mail); U.S. v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (same); In Re F.P., a Minor, 878 A.2d 91, 94 (Pa. Super. Ct. 2005) (transcripts of instant messaging conversation authenticated based on defendant's screen name, use of defendant's first name, and content of threatening message, which other witnesses had corroborated); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1153-54 (C.D. Cal. 2002) (admitting website postings as evidence due to circumstantial indicia of authenticity, including dates and presence of identifying web addresses).

On the other hand, just confronting the witness with their own social network postings may be sufficient. In Clark v. Indiana (2009) 915 N.E.2d 126, the defendant in a criminal case was confronted on the witness stand with his boasts on his MySpace page. This was upheld on appeal as evidence relevant to impeach his character and his defense.

RELEVANT CALIFORNIA AND FEDERAL STATUTES

Anyone considering accessing another's computer, had best be aware of the criminal statutes, state and federal, that preclude **un**authorized access.

I. CALIFORNIA LAW

PENAL CODE § 502(c)

...(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:...

(2) Knowingly **accesses and without permission takes, copies, or makes use** of **any data from a computer**, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. (Italics added.)

There is an exemption to this statute for those who have authorization. Section (h) states: "(1) Subdivision (c) does not apply to punish any acts which are committed by a person within the scope of his or her lawful employment. For purposes of this section, a person acts within the scope of his or her employment when he or she performs acts which are reasonably necessary to the performance of his or her work assignment."

The punishment component of the section is found in (d):

(1) Any person who violates any of the provisions of paragraph (1), **(2),** (4), or (5) of subdivision (c) is punishable by a fine not exceeding twelve thousand dollars ($12,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

In situations where there is arguable access to another's computer, the courts often look to measures taken by the owner to protect computer's contents. Password protection of files is often determinative of the expectation of privacy in computer files. Password protected files have been compared to a "locked footlocker inside the bedroom." Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001). In Trulock roommates both used a computer located in one bedroom and each had joint access to the hard drive. Both protected their personal files with passwords; and did not have access to each other's passwords. Although one roommate had authority to consent to a general search of the computer, her authority did not extend to other roommate's password-protected files.

Note that hacking into Facebook or other social media of another can be identity theft. In re Rolando S. (2011) 197 Cal.App.4th 936, the minor accessed the victim's Facebook account, altered her profile, and posted obscene messages and comments purporting to come from the victim. The appeals court upheld the finding that this violated PC §530.5(a), identity theft.

Penal Code § 11166. Duty to report; Mandated reporters; Punishment for violation[12]

"(e)(1) Any commercial film, photographic print, or image processor who has knowledge of or observes, within the scope of his or her professional capacity or employment, any film, photograph, videotape, negative, slide, or any representation of information, data, or an image, including, but not limited to, any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disk, data storage medium, CD-ROM, computer-generated equipment, or computer-generated image depicting a child under 16 years of age engaged in an act of sexual conduct, shall immediately, or as soon as practically possible, telephonically report the instance of suspected abuse to the law enforcement agency located in the county in which the images are seen. Within 36 hours of receiving the information concerning the incident, the reporter shall prepare and send, fax, or electronically transmit a written followup report of the incident with a copy of the image or material attached.

(2) **Any commercial computer technician** who has knowledge of or observes, within the scope of his or her professional capacity or employment, any representation of information, data, or an image, including, but not limited, to any computer hardware, computer software, computer file, computer floppy disk, data storage medium, CD-ROM, computer-generated equipment, or computer-generated image that is retrievable in perceivable form and that is intentionally saved, transmitted, or organized on an electronic medium, depicting a child under 16 years of age engaged in an act of sexual conduct, shall immediately, or as soon as practicably possible, telephonically report the instance of suspected abuse to the law enforcement agency located in the county in which the images or material are seen. As soon as practicably possible after receiving the information concerning the incident, the reporter shall prepare and send, fax, or electronically transmit a written followup report of the incident with a brief description of the images or materials."

---

[12] Typically, this provision applies to mental health professionals. But note the recent case of In re Elijah W. (2013) 216 Cal.App.4th 140, which holds that if such an expert is hired or appointed under the attorney client privilege, the privilege trumps the expert's statutory responsibility as a mandated reporter and the work remains confidential.

Computer Spyware-- Business & Professions Code section 22947 et seq.
This law prohibits an unauthorized person from knowingly installing or providing software that performs certain functions, such as taking control of the computer or collecting personally identifiable information, on or to another user's computer located in California.

Security Breach Notice - California Civil Code sections 1798.29, 1798.82, & 1798.84.
This law requires a business or a State agency that maintains unencrypted computerized data that includes personal information, as defined, to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The type of information that triggers the notice requirement is an individual's name plus one or more of the following: Social Security number, driver's license or California Identification Card number, financial account numbers, medical information or health insurance information. The notice must contain specific information, and any agency, person, or business that is required to issue a breach notice to more than 500 California residents must electronically submit a single sample copy to the Attorney General.

Online Privacy Protection Act of 2003, Bus. & Prof. Code §§ 22575-22579.
This law requires operators of commercial web sites or online services that collect personal information on California residents through a web site to conspicuously post a privacy policy on the site and to comply with its policy. The privacy policy must, among other things, identify the categories of personally identifiable information collected about site visitors and the categories of third parties with whom the operator may share the information. An operator is in violation for failure to post a policy within 30 days of being notified of noncompliance, or if the operator either knowingly and willfully or negligently and materially fails to comply with the provisions of its policy. This law took effect July 1, 2004.

Personal Information Collected on Internet - Government Code section 11015.5.
This law applies to state government agencies. When collecting personal information electronically, agencies must provide certain notices. Before sharing an individual's information with third parties, agencies must obtain the individual's written consent.

Public Officials, Online Privacy - Government Code 6254.21.
This law prohibits posting or displaying on the Internet the home address or telephone number of any elected or appointed official, as defined, if the official has made a written demand not to disclose his or her information. Entities receiving such a demand must remove the information immediately and ensure that it is not reposted.

Reproductive Health Care, Online Privacy - Government Code section 6218 et seq.
This law protects the personal safety of reproductive health care providers, employees, volunteers, and patients by prohibiting the posting of any such person's home address, phone number, or image on the Internet, under specified circumstances.

Safe at Home Participants, Online Privacy - Government Code sections 6206.5, 6206.7, 6208, 6215.3, 6215.4, 6215.7, 6208.1, 6208.2, and 6218.01.
This law provides participants in the Secretary of State's confidential address program, Safe at Home (for victims of domestic violence or stalking and reproductive health care providers, employees, and volunteers) with the right to demand the removal of their personal information, including home address and phone number, from online search engines or databases, and imposes related obligations on the operators of such search engines and databases.

II. FEDERAL STORED COMMUNICATIONS ACT (SCA)

In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA") "to afford privacy protection to electronic communications" by amending Title III to the Omnibus Crime Control and Safe Streets Act of 1968 (also known as the federal Wiretap Act). The latter only provided statutory protection to land-line "wire and oral communications." Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002). As part of the statutory measures to provide protection to electronic communications, Congress enacted as Title II to the ECPA the Stored Communications Act ("SCA"), which is "designed to 'address[] access to stored wire and electronic communications and transactional records." Id.

The SCA prohibits anyone "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service," or "divulg[ing] a record or other information pertaining to a subscriber or customer of such service." 18 U.S.C. § 2702(a). The Ninth Circuit has noted the statute at times is "ill-suited to address modem forms of communication," oftentimes requiring courts to "struggle[] to analyze problems involving modem technology within the confines of this statutory framework, often with unsatisfying results." Konop, 302 F.3d at 874.

Some of the provisions of the statute are:

18 U.S.C. § 2701. Unlawful access to stored communications
(a) Offense. Except as provided in subsection (c) of this section whoever--
(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; **or**

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.[13]

(b) Punishment. The punishment for an offense under subsection (a) of this section is-- (1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State--

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2) in any other case--

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(**c) Exceptions.** Subsection (a) of this section does not apply with respect to conduct authorized--

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title [18 USCS § 2703, 2704, or 2518].

§ 2711. Definitions for chapter

As used in this chapter [18 USCS §§ 2701 et seq.]--

(1) the terms defined in section 2510 of this title [18 USCS § 2510] have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" **means the provision to the public** of computer storage or processing services by means of an electronic communications

---

[13] *See e.g.,* Van Alstyne v. Elec. Scriptorium, Ltd. (4th Cir. 2009) 560 F.3d 199, a case where an employee successfully sued her employer for taking emails out of her password protected AOL account (not her company account but apparently on the company computer.)

system;[14]

(3) the term "court of competent jurisdiction" has the meaning assigned by section 3127 [18 USCS § 3127], and includes any Federal court within that definition, without geographic limitation; and

(4) the term "governmental entity" means a department or agency of the United States or any State or political subdivision thereof.

In Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121 (W.D. Wash. 2000), employees were "without authorization" to access information from their employer's computers when they began to appropriate the employer's tradesecrets for the benefit of the competitor. The court applied principles of agency law to conclude that the employees' authorized access to the employer's computers ended at the moment when they became agents of the competitor and began appropriating information from the employer's computer for the competitor's benefit.

III. COMPUTER FRAUD & ABUSE ACT (CFAA) 18 USC § 1030(A)(5)(A)

The "Computer Fraud and Abuse Act (CFAA), since its enactment in 1984, has continuously been broadened in scope and coverage. "[A]s new forms of computer crimes emerge, the CFAA will continue its evolution as courts construe and apply particular provisions of the statute." (Pac. Aero & Elects., Inc. v. Taylor (ED Wash. 2003) 295 F. Supp. 2d 1188, 1195 (discussing the history of the CFAA in detail.)

I. The Statute and its Elements

A. Generally

Section 1030 lists three types of offenses under (a)(5)(A) Each section subscribes a different mens rea for the resulting damage. It criminalizes conduct for whomever:

(A) (i) knowingly **causes the transmission of a program, information, code or command, and as a result of such conduct, intentionally causes damage** without authorization, to a protected computer;

(ii) **intentionally accesses a protected computer without authorization,**

---

[14] Hilderman v Enea TekSci, Inc. (2008 SD Cal) 551 F Supp 2d 1183, 27, holds the SCA does not apply to laptops. The court held it is questionable whether a laptop qualifies as a "facility through which an electronic communication service is provided." See Theofel v. Farey-Jones, 359 F.3d 1066, 1077 n. 4 (9th Cir. 2004) Setting that issue aside, the e-mail messages stored on the laptop's hard drive do not constitute "electronic storage" within the meaning of the SCA.

and as a result of such conduct, recklessly causes damage; or

(iii) **intentionally access a protected computer without authorization,** and as a result of such conduct, causes damage; and

(B) by conduct described above, caused

(i) loss to 1 or more persons during any 1-year period.... aggregating at least $5,000 in value.

"Section 1030 is general.... What protects people who accidentally erase songs on an iPod, trip over (and thus disable) a wireless base station, or rear-end a car and set off a computerized airbag, is not judicial creativity but the requirements of the statute itself: the damage must be intentional, it must be substantial... and the computer must operate in interstate or foreign commerce." (U.S. v. Mitra, 405 F.3d 492, 495-496 (7th Cir. 2005).)

18 USC § 1030(a)(5) criminalizes computer crime that damages natural persons and corporations. U.S. v. Middleton, 231 F.3d 1207, 1212-1213 (9th Cir. 2000). This section is "aimed at 'outsiders,' i.e., those lacking authorization to access any Federal interest computer." U.S. v. Morris, 928 F.2d 504, 510 (2d Cir. 1991).

B. Punishment

The punishment for an offenses under subsection (i), for individuals who intentionally causes damage, the punishment is a fine, imprisonment for not more than 10 years, or both. See § 1030(c)(4)(A).

For a violation of subsection (ii), for individuals who recklessly cause damage, punishment is a fine, imprisonment of not more than 10 years, or both. See § 1030(c)(4)(B).

Subsection (iii), an intentional access that causes damage, is a misdemeanor, punishable by a fine, imprisonment of not more than one year, or both. see § 1030(c)(2)(A).

II. DEFINITIONS

1. "Protected Computer"

A "protected computer" is either a computer 1) that is used in interstate or foreign commerce, (§ (e)(2)(B) or 2) is used exclusively by a financial institution or the United State Government, or a computer that's use by a financial institution or the United States Government has been affected by the offense conduct. (§ (e)(2)(A))

"[T]he statute does not ask whether the person who caused the damage acted in interstate commerce; it protects computers (and computerized communication systems) used in such commerce, no matter how the harm is inflicted." U.S. v. Mitra, 405 F.3d 492, 496 (7th Cir. 2005).

2. "Without authorization"

"Congress did not define the phrase 'without authorization,' perhaps assuming that the words speak for themselves. The meaning, however, has proven to be elusive." EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582, fn. 10 (1st Cir. 2001).

In U.S. v. Morris, 928 F.2d 504, 510 (2d Cir. 1991), the Court reasoned that "without authorization" is use that is not in any way related to its intended function.

"[A]lthough Congress did not define the phrase 'without authorization' in either the SECA or the CFAA, it did provide a statutory definition for the phrase 'exceeds authorized access' in the CFAA... [which] means 'to access a computer without authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter. 18 U.S.C. § 1030(e)(6).'" Int'l Ass'n of Machinists & Aero. Workers v. Werner-Matsuda, 390 F. Supp. 2d 479, 498 (Dist. Maryland 2005).

3. "Damage"

Means "any impairment to the integrity or availability of data, a program, a system or information." (§ 1030(e)(I)(8)). Instructing the jury that it could consider only those costs that were a "natural and foreseeable result" of the defendant's conduct, only those costs that were "reasonably necessary," and only those costs that would resecure the computer to avoid "further damage" is proper. "In particular, the term 'resecure' implies making the system as secure as it was before, not making it more secure that it was before." U.S. v. Middleton, 231 F.3d 1207, 1213 (9th Cir. 2000).

4. "Loss"

Means "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." (§ 1030(e)(i)(11). It is permissible for the court to compute "loss" based on the hourly wage of the victim bank's employees, because the bank would have had to pay a similar amount had it hired an outside contractor to repair the damage caused by the violation. U.S. v. Sablan, 92 F.3d 865, 869 (9th Cir. 1996).

5. The Drew Case

This was the so-called "cyber bully" case tried in federal court in Los Angeles. There, Ms. Drew, who resided in a St. Louis suburb, created a phony MySpace profile of a young boy who befriended a young neighbor girl on MySpace. The young girl lived only a few houses away from Drew, but because MySpace's office was in Beverly Hills,

the cyber transmission went from Drew's home near St. Louis to Los Angeles and back to the young girl's home a few doors away in St. Louis. Because the email traffic between the two turned ugly, the young girl committed suicide and Drew was prosecuted by the U.S. Attorney in Los Angeles for a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. Specifically, she was prosecuted under the provision that states whoever intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains information from any protected computer is guilty of a federal crime (assuming interstate/foreign communications were involved.) Punishment can be a misdemeanor or a felony for up to five years in prison if the offense was committed in furtherance of a crime or a tortious act.

In Drew, the government theory of "exceeding" authorized access was this: MySpace, like all social networks, has a detailed description of its "terms of service." These are similar to the End User License Agreements (EULA) we are so familiar with when beginning use of a program. Most of us ignore them, scroll to the bottom, say "I agree," and activate the service. With MySpace, several of the terms of service are: the user must agree to provide truthful registration information, must refrain from using MySpace to abuse or harm others and must not solicit information from persons under 18. Violation of these terms was deemed by the government to mean Drew exceeded the authorized access to the young girl's MySpace profile. In this sense, the MySpace terms of service were elevated to violations of the federal criminal statute.

In Ms. Drew's case, the government charged felony conspiracy and substantive felonies for several of the MySpace contacts with the girl. The basis of the felony was that Drew committed a tortious act – the intentional infliction of mental distress. Thanks to the hard work of Dean Steward, she was acquitted of the felonies and convicted of several misdemeanors. Thereafter, the trial judge dismissed the misdemeanors. See U.S. v. Drew, 259 F.R.D. 449 (C.D. Ca. 2009).

6. United States v. Nosal, 676 F.3d 854 (9th Cir. 2012). The defendant was charged with violations of 18 U.S.C. § 1030(a)(4), for aiding and abetting his former coworkers in *"exceeding their authorized access"* to their employer's computers, with intent to defraud. The court determined that the government's statutory interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute. The term "entitled" in the statutory text referred to how an accesser obtained or altered the information, whereas the employer's computer use policy used "entitled" to limit how the information was used after it was obtained. The court concluded that this was a poor fit with the statutory language. An equally and more sensible reading of "entitled" was as a synonym for "authorized." So read, "exceeds authorized access" would refer to data or files on a computer that one was *not authorized*

to access. Invoking the rule of lenity, the court had to choose the interpretation least likely to impose penalties unintended by Congress. "We remain unpersuaded by the decisions of our sister circuits that interpret the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty." (Id. at 862.) "[W]e hold that the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions." (Id. at 863.)

IV. Electronic Communications Privacy Act §§ 2702(a)(1), 2510(15), § 2510(13).

An email service provider is not compelled to produce documents under a § 1782 order (an order to obtain evidence for use in a foreign or international tribunal). Suzlon Energy Ltd. sought discovery of the emails of an Indian citizen from Microsoft Corp., a US based email service provider, for use in an Australian court proceeding. Under 28 U.S.C § 1782, a party may petition a district court for discovery for use in a foreign proceeding. The district court granted Microsoft's motion to quash Suzlon's § 1782 petition and refused Suzlon the emails. The Ninth Circuit held that despite the numerous statutory exceptions to the prohibition on an email service provider from divulging the contents of an electronic communication under § 2702(a)(1) of the Electronic Communications Privacy Act (ECPA), Congress provided no exceptions for citizenship, and the plain language of § 2510(13) of the ECPA protects "any person" which includes foreign citizens. AFFIRMED. **Suzlon Energy v. Microsoft Corporation Date Filed: (9th Cir. 10/3/11** Case No: 10-35793)

TECH RELATED CALIFORNIA STATE BAR OPINIONS

Abstracts of The State Bar of California Standing Committee on Professional Responsibility and Conduct Formal Opinion Number. The full opinion may be found at http://ethics.calbar.ca.gov/Ethics/Opinions/2009176toPresent.aspx

No. 2013 188: Q. If an attorney receives from a non-party a confidential written communication between opposing counsel and opposing counsel, what should the attorney do if the attorney reasonably believes that the communication may not be privileged because of the crime-fraud exception to the attorney-client privilege?

A. If an attorney receives an unsolicited intentionally transmitted written communication between opposing counsel and opposing counsel's client under circumstances reasonably suggesting that it is a confidential communication apparently sent without the consent of its owner, the attorney may not ethically read the communication, even if she suspects the crime-fraud exception might vitiate the privilege. The attorney must notify opposing counsel as soon as possible that the attorney has possession of the communication. The two attorneys should try to resolve the privilege issue or, if that fails, obtain the assistance of a court. Attorney may not read, disseminate, or otherwise use the communication or its contents absent court approval or consent of its owner.

No. 2012 186: Q. Under what circumstances would an attorney's postings on social media websites be subject to professional responsibility rules and standards governing attorney advertising?

A. Material posted by an attorney on a social media website will be subject to professional responsibility rules and standards governing attorney advertising if that material constitutes a "communication" within the meaning of rule 1-400 (Advertising and Solicitation) of the Rules of Professional Conduct of the State Bar of California; or (2) "advertising by electronic media" within the meaning of Article 9.5 (Legal Advertising) of the State Bar Act.[15] The restrictions imposed by the professional

---

[15] *See* the recent case of Steiner v. Superior Court (Volkswagen Group of America) 2013 Cal. App. Unpub. LEXIS 7835 (October 30, 2013), in which the court voided an order to an attorney to take down from the firm's website two case descriptions of successes that were similar to the case at issue. This was held a First Amendment violation as a prior restraint, but the court explicitly said it was not ruling on a Rule of Professional Conduct in "criminal proceedings." (See Gentile v. Nevada (1991) 501 U.S. 1030, authorizing such restrictions in a criminal case context.)

responsibility rules and standards governing attorney advertising are not relaxed merely because such compliance might be more difficult or awkward in a social media setting.

No. 2012 184: Q. Ethical obligations, if the communications with the client, and storage of and access to all information about the client's matter, are all conducted solely through the internet using the secure computer servers of a third-party vendor (i.e., "cloud computing")?

A. As it pertains to the use of technology, the Business and Professions Code and the Rules of Professional Conduct do not impose greater or different duties upon a VLO [Virtual Law Office] practitioner operating in the cloud than they do upon an attorney practicing in a traditional law office. While an attorney may maintain a VLO in the cloud where communications with the client, and storage of and access to all information about the client's matter, are conducted solely via the internet using a third-party's secure servers, Attorney may be required to take additional steps to confirm that she is fulfilling her ethical obligations due to distinct issues raised by the hypothetical VLO and its operation. Failure of Attorney to comply with all ethical obligations relevant to these issues will preclude the operation of a VLO in the cloud as described herein.

No. 2010-179: Q. Does an attorney violate the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties?

A. Whether an attorney violates his or her duties of confidentiality and competence when using technology to transmit or store confidential client information will depend on the particular technology being used and the circumstances surrounding such use. Before using a particular technology in the course of representing a client, an attorney must take appropriate steps to evaluate: 1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the situation; and 6) the client's instructions and circumstances, such as access by others to the client's devices and communications.

No. 2007 174: Q. Is an attorney ethically obligated, upon termination of employment, promptly to release to a client, at the client's request, (1) an electronic version of e-mail correspondence, (2) an electronic version of the pleadings, (3) an electronic version of

discovery requests and responses, (4) an electronic deposition and exhibit database, and/or (5) an electronic version of transactional documents?

A. An attorney is ethically obligated, upon termination of employment, promptly to release to a client, at the client's request: (1) an electronic version of e-mail correspondence, because such items come within a category subject to release; (2) an electronic version of the pleadings, because such items too come within a category subject to release; (3) an electronic version of discovery requests and responses, because such items are subject to release as reasonably necessary to the client's representation; (4) an electronic deposition and exhibit database, because such an item itself contains items that come within categories subject to release; and (5) an electronic version of transactional documents, because such items are subject to release as reasonably necessary to the client's representation. The attorney's ethical obligation to release any electronic items, however, does not require the attorney to create such items if they do not exist or to change the application (e.g., from Word (.doc) to WordPerfect (.wpd)) if they do exist. Prior to release, the attorney is ethically obligated to take reasonable steps to strip from each of these electronic items any metadata reflecting confidential information belonging to any other client.

No. 2005 168: Q. Does a lawyer who provides electronic means on his web site for visitors to submit legal questions owe a duty of confidentiality to visitors who accept that offer but whom the lawyer elects not to accept as clients, if the attorney disclaims formation of an attorney-client relationship and a "confidential relationship"?

A. A lawyer who provides to web site visitors who are seeking legal services and advice a means for communicating with him, whether by e-mail or some other form of electronic communication on his web site, may effectively disclaim owing a duty of confidentiality to web-site visitors only if the disclaimer is in sufficiently plain terms to defeat the visitors' reasonable belief that the lawyer is consulting confidentially with the visitor. Simply having a visitor agree that an "attorney-client relationship" or "confidential relationship" is not formed would **not** defeat a visitor's reasonable understanding that the information submitted to the lawyer on the lawyer's web site is subject to confidentiality. In this context, if the lawyer has received confidential information from the visitor that is relevant to a matter in which the lawyer represents a person with interests adverse to the visitor, acquisition of confidential information may result in the lawyer being disqualified from representing either.

No. 2001 155: Q. What aspects of professional responsibility and conduct must an attorney consider when providing an Internet web site containing information for the public about her availability for professional employment?

A. An attorney's Internet web site providing to the public information about her availability for professional employment is a "communication" under rule 1-400(A) of the Rules of Professional Conduct and an "advertisement" under Business and Professions Code sections 6157 to 6158.3. As such, it is subject to the applicable prohibitions on false, misleading, and deceptive messages. The content of the pages constituting the web site must be prepared carefully to satisfy these rules. This applies to the words that make up the message and to the images and sounds which are part of the presentation. Under the facts presented, the web site is not a "solicitation" under rule 1-400(B) even if it includes electronic mail facilities allowing direct communication to and from the attorney. The attorney also must be aware of the possibility that the web site might be subject to regulation by other jurisdictions or that it might be considered the unauthorized practice of law in other jurisdictions.

HAVE YOU BEEN WIRETAPPED RECENTLY?

Chuck Sevilla

[this was written 8 years ago and sets forth the wiretap laws and how they may apply to purely domestic government eavesdropping]

A. The Problem. The revelation in last Friday's New York Times (12/16/05) that the government authorized the National Security Agency to commence surveillance of domestic communications involving foreign contacts may reveal an overwhelming abuse of power. In fact, the very authorization appears to be an abuse of power given that domestic surveillance is specifically limited by two controlling statutes.

In the wake of 9/11, many of us were giving advice to Muslim people living in our communities who had been contacted by the FBI. Was that enough justification for the government to tap our phones and read our email? We don't know. We don't know if records were kept of the taps, or what procedures within the National Security Agency existed to justify the spying. The agency is enormous. It is three times bigger than the CIA. It has a lot of resources to use on electronic spying. In fact, that's all it does.

The laws on electronic eavesdropping are quite specific as to how it may be done. Title III of the Omnibus Crime Control and Safe Street Act of 1968 (18 U.S.C. §§ 2510 *et seq.*) prohibits recording oral communications when the person exhibits "an expectation that such communication is not subject to interception under circumstances justifying such expectation." (18 U.S.C. §§ 2510(2), 2515.) This Act was aimed at permitting limited domestic electronic surveillance when authorized by a judicial warrant based on probable cause.

The Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. 1801 *et seq,* was passed to permit the government surveillance of domestic communications involving the capture of foreign intelligence. It was quite generous in allowing the government to "tap first, and justify later" with the FISA court. Out of the thousands of requests, reportedly the government has been turned down only a few times. For targets who are "United States persons," the FISA court must find on the basis of the facts submitted by the government that there is probable cause to believe the target of the electronic surveillance is a foreign power or an agent of a foreign power, but no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the First Amendment.

It is a federal felony to surveil domestically without compliance of either of the

two statutes. 50 U.S.C. 1809 states that "a person is guilty of an offense if he intentionally—(1) engages in electronic surveillance under color of law except as authorized by statute." The crime is punishable by a fine and five years in prison.

B. The Purported Justifications. So far, the President says his authorization to N.S.A. to conduct this surveillance is justified by: 1) his constitutional powers as Commander in Chief; 2) the fact that Congress authorized him to make war on Iraq and Afghanistan; and 3) because he notified a few leaders in Congress about what he was authorizing. The later two rationales do not pass the smell test. The justification to make war has never been deemed a *carte blanche* to void the Fourth Amendment to the Constitution and invade the privacy of the citizenry. Second, talking to a selected few Congressmen has never excused bypassing existing legislation.

The Commander in Chief argument was rejected as justifying warrantless domestic spying in U.S. v. U. S. Dist. Court 407 U.S. 297 (1972). There, the Supreme Court rejected the President's argument in a case involving a defendant charged with dynamite bombing of a CIA office. The defendant sought discovery of electronic surveillance information and for a hearing to suppress it if illegally obtained. The surveillance had been conducted without prior judicial approval, but the government argued domestic eavesdropping was lawful as a reasonable exercise of the President's power to protect the national security. The Supreme Court rejected the argument and held that the surveillance violated the Fourth Amendment. It held prior judicial approval was required for the type of domestic security surveillance and that such approval could be made in accordance with such reasonable standards as Congress prescribed in Title III. "These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch. (Id. at 316-317.)

The President now argues that the above case only dealt with purely domestic warrantless spying, and that the N.S.A. only captures domestic communications linked to a foreign source. However, in 1978, Congress passed the FISA law to give the government generous powers to tap domestic subversives believed to be operating for foreign powers. That legislatively covered the President's current argument to permit the unmonitored spying N.S.A. has been doing these past four years.

The FISA power was not good enough, says the Administration, because it is not suited to the technological advances used by terrorists today. Given the existing legislation that prohibits unilateral government eavesdropping on U.S. citizens, an alternative for the Administration would have been to go to the Republican Congress and seek legislative authorization for the augmented power it deemed necessary. Instead, Bush chose to unilaterally assume that power and not to tell anyone about it except a few

chosen ones in Congress. (What they were told is another matter as Senator Rockefeller has recently disputed that he was provided sufficient detail or that he approved.)

The government assures us that this surveillance power was used modestly, justified by intelligence, and was needed to protect Americans from terrorist attack. Consider this: we have no way to find out the truth of any of these justifications. Further, it was the same government intelligence that led to the preemptive war in Iraq in 2003. It was based upon three major justifications: Iraq's alleged possession of WMDs, its alleged terrorist connections to al-Qaeda, and its alleged building nuclear threat. All false.

Only this month, the President acknowledged the intelligence was wrong. Now, we are asked to trust his government's representations that the spying these last four years has been reasonably based on the same government intelligence.

In a nation founded upon constitutional checks and balances, there is neither a check nor a balance to this unilateral exercise of power. As defense attorneys we have experienced the governmental abuse of powers lawfully given. Here, it has granted itself unrestricted, unregulated and unmonitored powers to spy on us, and exercised them in secret for years. That is the chemistry for abuse.

C. What Can Be Done? It has only been one week since we learned this surveillance has been on-going for over four years. We have to insist that Congress hold hearings to discover just how widespread the tapping was, and how extensive the abuse. Just yesterday, the N.Y. Times reported "accidental" captures of purely domestic communications. ***How come I have a feeling that if the truth is ever revealed we will learn of a massive governmental spying operation on purely domestic communications?*** Those of us who lived during Watergate learned how unchecked Presidential power corrupts. An Administration that can justify the legality of torture, can rationalize any usurpation of power.

Attorneys with pending cases should bring motions to require the government to disgorge whether the client or the attorney has been tapped by the government. In federal cases, a discovery motion should be made to ask for information about any kind of electronic surveillance pursuant to 18 U.S.C. § 2510 et seq., § 3504, and 50 U.S.C. § 1806.

One could also make a "FOIA" request under the Administrative Procedures Act, 5 U.S.C. Section 552 et. seq., the Freedom of Information Act, seeking the disclosure of documents from the N.S.A. on government surveillance of one's email and phone conversations. I'm not an expert on that process and know that the government would

assert an exemption that disclosure would expose techniques and procedures for law enforcement investigations or prosecutions. That battle will take years.

Finally, if there were ever a time to emphasize that substantive client conversations should take place in the confidentiality of an office interview or at the jail, and not on the phone or by email, this is it.

If you are lucky enough to learn of the use of the Bush surveillance in your own cases, please let us know so that we may be informed and follow your lead.

ANSWER: YES YOU HAVE

[*The following is a collection of recent materials on the Snowden - NSA Revelations*]

Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence
By CHARLIE SAVAGE Published: October 26, 2013 NY Times

WASHINGTON — The Justice Department for the first time has notified a criminal defendant that evidence being used against him came from a warrantless wiretap, a move that is expected to set up a Supreme Court test of whether such eavesdropping is constitutional.

Solicitor General Donald B. Verrilli Jr. said defendants had a right to know if prosecutors had relied on wiretaps. Prosecutors filed such a notice late Friday in the case of Jamshid Muhtorov, who was charged in Colorado in January 2012 with providing material support to the Islamic Jihad Union, a designated terrorist organization based in Uzbekistan.

Mr. Muhtorov is accused of planning to travel abroad to join the militants and has pleaded not guilty. A criminal complaint against him showed that much of the government's case was based on intercepted e-mails and phone calls.

The government's notice allows Mr. Muhtorov's lawyer to ask a court to suppress the evidence by arguing that it derived from unconstitutional surveillance, setting in motion judicial review of the eavesdropping.

The New York Times reported on Oct. 17 that the decision by prosecutors to notify a defendant about the wiretapping followed a legal policy debate inside the Justice Department.

The debate began in June when Solicitor General Donald B. Verrilli Jr. discovered that the department's National Security Division did not notify criminal defendants when eavesdropping without a warrant was an early link in an investigative chain that led to evidence used in court. As a result, none of the defendants knew that they had the right to challenge the warrantless wiretapping law.

The practice contradicted what Mr. Verrilli had told the Supreme Court last year in a case challenging the law, the FISA Amendments Act of 2008. Legalizing a form of the Bush administration's program of warrantless surveillance, the law authorized the government to wiretap Americans' e-mails and phone calls without an individual court order and on domestic soil so long as the surveillance is "targeted" at a foreigner abroad.

A group of plaintiffs led by Amnesty International had challenged the law as unconstitutional. But Mr. Verrilli last year urged the Supreme Court to dismiss the case because those plaintiffs could not prove that they had been wiretapped. In making that argument, **he said a defendant who faced evidence derived from the law would have proper legal standing and would be**

notified, so dismissing the lawsuit by Amnesty International would not close the door to judicial review of the 2008 law. The court accepted that logic, voting 5-to-4 to dismiss the case.

In a statement, Patrick Toomey, staff attorney with the American Civil Liberties Union, which had represented Amnesty International and the other plaintiffs, hailed the move but criticized the Justice Department's prior practice.

"We welcome the government's belated recognition that it must give notice to criminal defendants who it has monitored under the most sweeping surveillance law ever passed by Congress," Mr. Toomey said. "By withholding notice, the government has avoided judicial review of its dragnet warrantless wiretapping program for five years."

The Justice Department change traces back to June, when The Times reported that prosecutors in Fort Lauderdale and Chicago had told plaintiffs they did not need to say whether evidence in their cases derived from warrantless wiretapping, in conflict with what the Justice Department had told the Supreme Court.

After reading the article, Mr. Verrilli sought an explanation from the National Security Division, whose lawyers had vetted his briefs and helped him practice for his arguments, according to officials with knowledge of the internal deliberations. It was only then that he learned of the division's practice of narrowly interpreting its need to notify defendants of evidence "derived from" warrantless wiretapping.

There ensued a wider debate throughout June and July, the officials said. National security prosecutors raised operational concerns: disclosing more to defendants could tip off a foreign target that his communications were being monitored, so intelligence officials might become reluctant to share crucial information that might create problems in a later trial.

Mr. Verrilli was said to have argued that there was no legal basis to conceal from defendants that the evidence derived from legally untested surveillance, preventing them from knowing they had an opportunity to challenge it. Ultimately, his view prevailed and the National Security Division changed its practice going forward, leading to the new filing on Friday in Mr. Muhtorov's case.

Still, it remains unclear how many other cases — including closed matters in which convicts are already service prison sentences — involved evidence derived from warrantless wiretapping in which the National Security Division did not provide full notice to defendants, nor whether the department will belatedly notify them. Such a notice could lead to efforts to reopen those cases.

Correction: October 27, 2013
An earlier version of this article incorrectly stated that a criminal complaint showed that much of the government's case against Jamshid Muhtorov was based on e-mails and phone calls intercepted under a 2008 surveillance law. The complaint does not say that the particular communications it cites were obtained directly from such surveillance.

PRISM already gave the NSA access to tech giants. Here's why it wanted more.
By Andrea Peterson October 30, 2013 Washington Post

General Keith Alexander (2nd L), director of the National Security Agency (NSA) testifies at a House Intelligence Committee hearing on Capitol Hill in Washington October 29, 2013. Top U.S. intelligence officials appeared at a congressional hearing on Tuesday amid a public uproar that has expanded from anger over the National Security Agency collecting the phone and email records of Americans to spying on European allies. Alongside Alexander are NSA Deputy Director Chris Inglis (L), U.S. Director of National Intelligence James Clapper (2nd R) and Deputy Attorney General James Cole. General Keith Alexander, director of the NSA, testifies at a House Intelligence Committee hearing on Capitol Hill in Washington October 29, 2013.

A new report from the Post's Barton Gellman and Ashkan Soltani reveals that the **NSA has been tapping into the primary communications links that connect Yahoo and Google data centers around the world. That allowed the agency to collect metadata and content from hundreds of millions of user accounts -- including many belonging to American citizens and residents.**

The NSA already had robust front door access to those companies via PRISM. So why did it need a back door?

There are some obvious reasons: The operations take place overseas, where many statutory restriction on surveillance don't apply -- and where the Foreign Surveillance Intelligence Court (FISC) has no jurisdiction. In fact, the FISC ruled a similar, smaller scale program involving cables on U.S. territory illegal in 2011. So if the NSA decides to harvest that data on foreign soil, it can skip most of the oversight mechanisms.

Data are an essentially global commodity, and the backup processes of companies often mean that data is replicated many places across the world. So just because you sent an e-mail in the U.S., doesn't mean it will always stay within the nation's borders for its entire life in the cloud.

The PRISM program, revealed earlier this year by the Post and the Guardian, provided the NSA access to huge volumes of online communications from nine technology companies including Yahoo and Google by legally compelling them to turn over data matching court-approved search terms. Just yesterday, NSA chief Gen. Keith B. Alexander defended tech companies role in the PRISM program during a House Intelligence Committee hearing. "We have compelled industry to help us in this manner by court order," he argued, "and what they're doing is saving lives."

But the NSA may have preferred its back-door method of accessing the data because it was less visible to the technology companies holding the data. By accessing data without the knowledge of tech companies, it didn't have to worry that the volume of data iit was accessing could raise privacy alarm bells within those companies.

Both Yahoo and Google expressed concern about Gellman and Soltani's revelations and claimed the data link infiltration was done without their knowledge. In a statement to the Post, Google said it was "troubled" by the allegations and they were "not aware of this activity." Similarly, a Yahoo spokeswoman said the company had "not given access to our data centers to the NSA or to any other government agency."

Of course, it's also possible that the decision to collect the data wasn't part of any broader strategy. The NSA's mission is to collect and analyze foreign intelligence. Here, it had an opportunity to parse through a truly astounding amount of data. **Over one 30-day period earlier this year, the agency collected 181,280,466 new records, including metadata and the actual content of e-mails.** Scooping up data is deep in the NSA's DNA, and it may simply have been unable to help itself.

\\

Supreme Court Case: Four Months Too Soon

James R. Clapper, Jr., Director of National Intelligence, et al., v. Amnesty International USA et al, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (Feb. 26, 2013)

This case was brought by human-rights researchers and by lawyers who feared that because their foreign clients were plausible targets of surveillance, their own communications had quite likely been intercepted. The 5-to-4 majority dismissed the case for lack of standing. The majority holds that the plaintiffs cannot show "standing," that is, that they have been surveilled. (**If this case had only been decided a few months later!**) The case centers on the Foreign Intelligence Surveillance (FISA) Act Section 702, 50 U.S.C. §1881a, added by FISA Amendments Act which creates new procedures for authorizing electronic surveillance targeting non-U.S. persons abroad. Justice Alito wrote for the majority that the plaintiff's can only **speculate** as to whether government will seek to use Section 1881a-authorized surveillance, rather than other methods, and thus cannot satisfy standing requirements that they will suffer injury that is "fairly traceable" to challenged amendment.

This of course was written before the NSA revelations started rolling out this summer showing that nearly every electronic form of communication is gobbled up by the NSA. Standing was now seems presumptively established for anyone on earth given that NSA and its agents are monitoring people all over the earth.

By the way, as the Clapper dissent notes, the amendment to § 1881a in 2008 changed this prior law in three important ways. First, **it eliminated the requirement that the Government describe to the court each specific target** and identify each facility at which its surveillance would be directed, thus permitting surveillance on a programmatic, not necessarily individualized, basis. § 1881a(g). Second, **it eliminated the requirement that a target be a "foreign power or an agent of a foreign power."** Third, **it diminished the court's authority to insist upon, and eliminated its authority to supervise, instance-specific privacy-intrusion** minimization procedures (though the Government still must use court-approved general

minimization procedures). § 1881a(e). Thus, using the authority of § 1881a, the Government can obtain court approval for its surveillance of electronic communications between places within the United States and targets in foreign territories by showing the court (1) that "a significant purpose of the acquisition is to obtain foreign intelligence information,"and (2) that it will use general targeting and privacy-intrusion minimization procedures of a kind that the court had previously approved. § 1881a(g).

Senator Ron Wyden (D-Ore.) explains, "Once Americans' communications are collected, a gap in the law ... allows the government to potentially go through these communications and conduct warrantless searches for the phone calls or emails of law-abiding Americans."

The Guardian published three FISA Court documents outlining the NSA's procedures for minimizing its collection of domestic communications. Among the most controversial revelations in the files is that the **NSA can store domestic communications if they contain:** 1) foreign intelligence information; 2) **evidence of a crime;** 3) threats of serious harm to life or property; 4) or any other information that could aid the agency's electronic surveillance, which includes encrypted communications.

Defense Lawyers Insist on Clients' Right to Use NSA records
(Miami Herald, by Alfonso Chardy Posted on Sun, Aug. 18, 2013)

On a stretch of North Federal Highway in Lighthouse Point sits a branch of Bank of America.

The location, at the corner of Northeast 29th Street near Pompano Beach, is at the heart of a landmark motion filed recently in Fort Lauderdale federal court that sought phone records from the National Security Agency (NSA) in a South Florida criminal case.

In the fallout over NSA leaker Edward Snowden's revelations, one of the unintended consequences is a sudden interest on the part of many defense lawyers across the nation to seek agency records that could help their clients in ordinary criminal cases.

U.S. officials have acknowledged in the wake of Snowden's leaks that for years the NSA has collected and stored vast amounts of telephone and email records as part of its strategy to detect potential terrorist attacks against the United States.

One of the first phone-records motions in a criminal case came from Marshall Dore Louis, a Miami defense attorney who represents **Terrance Brown**, implicated in a federal bank truck robbery conspiracy case. Dore may have started a trend.

After Dore filed his motion in June, he received calls and email messages from dozens of attorneys across the country interested in filing similar motions in their cases.

In addition, many more attorneys in drug-trafficking cases nationwide are said to be preparing motions after Reuters revealed on Aug. 5 that the NSA is a partner in a special Drug Enforcement Administration (DEA) unit that supplies tips to local law-enforcement authorities. Those tips come from a massive phone-records database that the DEA's Special Operations Division (SOD) taps, Reuters said.

The expected onslaught of demands for NSA records from defense attorneys is an ironic twist for a once-secretive agency whose acronym was often jokingly said to stand for No Such Agency.

Brown was recently convicted of only one of the nine counts in a case stemming from a deadly Oct. 1, 2010, robbery that unfolded when a Brinks truck was delivering $397,500 to a Bank of America branch in Miramar. The government has yet to decide whether it will retry Brown on the eight counts upon which the jury could not reach a verdict.

Brinks worker Alejandro Nodarse Arencibia of Hialeah, 48, was killed when one of the robbers — not Brown — shot him in the head as he walked to the bank with a bag containing the money.

While that robbery has been the focus of media attention since Dore filed his motion in June, his demand for NSA records actually focused on an earlier episode — July 26, 2010 — when federal

prosecutors allege that his client was at or near the Bank of America branch at Lighthouse Point waiting for a money truck to arrive.

No robbery occurred because the truck never showed up, but Brown was still linked to the conspiracy because prosecutors insisted he was in the area. As evidence, they cited phone calls to him from alleged accomplices but did not produce any phone records showing he was positively there.

“The government was asserting that my client was in Lighthouse Point, Fla., attempting to rob a bank in July, but they did not have location data for the phone that they alleged was his,” Dore said in an interview Wednesday. “So, they did have it for people that they alleged were in the conspiracy, but not my client.”

After reading an article in The Guardian newspaper in early June about Snowden’s leaks about NSA phone- and email-collection programs, Dore hit upon the idea that the agency likely possessed cellphone location data for his client.

According to the Guardian and other media outlets, information from Snowden indicates that the NSA has become a sort of vast repository for intercepted communications — including phone-location records.

On June 9, Dore filed his motion in the hopes of finding evidence that would show his client was not in the vicinity of the bank at Lighthouse Point, as the government had alleged.

“The government must be ordered to turn over the records for the two telephones that it attributes to Mr. Brown for the dates which are relevant to this case — the month of July 2010,” Dore’s motion said. “The records for the two telephone numbers are in the government’s possession. The NSA operates under the authority of the United States Department of Defense, an arm of the executive branch of government.”

A day after Dore filed his motion, U.S. District Court Judge Robin Rosenbaum ordered the federal government to respond. On June 19, prosecutors filed a motion denying that the federal government had the location data that Dore sought.

Dore said in an interview on Wednesday that he has since withdrawn the motion because he is confident that Michael Mullaney, chief of the counterterrorism section of the Justice Department’s national security division, who represented that the records did not exist, would not make a misrepresentation to the court.

But his motion stirred the interest of other lawyers.

“I received a lot of contacts from other lawyers who wanted to get the information because, for the same reasons that it’s useful to the government, it’s useful to defense lawyers,” Dore said.

One of the lawyers who contacted Dore was John Steakley in Cobb County, Ga., where he represents a client in a double homicide case.

“I have a double homicide where witnesses called each other upon hearing gunshots,” Steakley said in an e-mail to El Nuevo Herald. “If those calls took place before my client arrived in the area [we have his records], then he couldn’t have done the shooting. I’ve tried to get the records of those phone calls, but the cell companies no longer have the records. If the NSA has been stockpiling the data, I’d like to get it.”

Steakley said on Thursday that he plans to file a motion demanding NSA phone records for those calls.

More lawyers became interested in filing motions after Reuters broke the story on the DEA’s unit to combat drug-trafficking Latin American cartels through a partnership with the NSA and other federal agencies that include the CIA, Homeland Security, the FBI and the Internal Revenue Service (IRS).

The DEA’s **Special Operations Division’s** practice of feeding tips on suspects to local law enforcement has drawn criticism because the initial source of the information, possibly NSA intercepts of phone data, has not been revealed when cases reach the courts.

According to Reuters, the original tip was concealed from judges, prosecutors and defense attorneys because of the classified nature of the unit. The tip generally was relayed to a state trooper who was told by investigators to search a specific vehicle in which drugs would be found.

In court, investigators would say that the case began with the vehicle search, not the SOD tip. Investigators called the procedure **parallel construction.**

The subterfuge has upset some legal experts who feel that court cases in which the practice was used have been compromised.

“I have never heard of it before,” Nancy Gertner, a Harvard law professor and former federal judge and defense lawyer, recently told the news show The Takeaway on National Public Radio. “I was a criminal defense lawyer for 24 years and a judge for 17, and I have never heard of this before. And yes, there were cases that began with traffic stops … I never saw anything that smacked of parallel construction.”

GLOSSARY OF SNOWDEN REVELATIONS ABOUT THE NSA[16]

"Any society that would give up a little liberty to gain a little security will deserve neither and lose both." – Ben Franklin

PRISM NSA has direct access via the PRISM program to the servers of some of the biggest U.S. tech companies, including Apple, Google and Microsoft. The Guardian revealed how large tech companies have worked closely with the NSA to help them circumvent encryption and other privacy controls, and how the agency pays for many of these companies' compliance costs. The Washington Post revealed that the NSA spends hundreds of millions of dollars each year paying private companies for access to large fiber optic communications backbones - part of the agency's **Corporate Partner Access Project**.

In an article not directly related to the NSA documents leaked by Edward Snowden - but thematically similar - The New York Times reveals that in 2008 the internet company Skype started a secret program to make Skype calls accessible to intelligence agencies and law enforcement. As the Times notes, documents leaked by Snowden confirm that Skype then joined the PRISM program in February 2009.

The Washington Post reported that as of April 5, 2013 there were 117,675 active surveillance targets—who must be foreign nationals overseas at the time of collection—in the PRISM database. The Post notes this number does not reveal how many other users—including Americans—may have had their information incidentally collected while the NSA was collecting information on these targets. Also, the NSA receives "real-time notification of an email-event, such as a login or sent message" as well as "real-time notification of a chat login or logout," according to the Post.

NSA program called **Upstream** collects information from the fiber optic cables that carry most Internet and phone traffic. The coverage is based on a PRISM.

The New York Times reports that the NSA uses Americans' data — including phone and email metadata, as well as information from social media and financial transactions — **to create maps of targets' social connections.** According to an agency spokesperson, this data is only used when there is "a foreign intelligence justification."

Boundless Informant, an NSA tool that provides "near real-time" statistics on the agency's spying capabilities and is broken down by country. Among the information the slides reveal is that the NSA collected almost 3 billion pieces of intelligence on U.S. citizens in February 2013 alone.

---

[16] The data here is from an excellent article in Aljazeera's timeline of the revelations. See http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html

Evil Olive, run by the NSA's Special Source Operations (SSO) department, revealed by The Guardian collects vast quantities of online metadata. One such program, **Shell Trumpet**, had collected 1 trillion metadata records as of December 2012. Another, **Transient Thurible**, passes online metadata collected by Britain's GCHQ into the NSA's systems. NSA has been using the **"Fairview"** program to gain access to the Internet and telephone data of foreign citizens - including Brazilians - through foreign telecoms' partnerships with American telecoms. It is estimated that **NSA stores 1 billion cellphone calls daily.**

XKeyscore data collection network of NSA. This NSA program has a network of 500 servers scattered across the globe that collect "nearly everything a user does on the Internet" and store it in databases searchable by name, email, IP address, region and language.

Follow the Money performs bulk data collection on international networks belonging to Visa, Mastercard, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and other financial institutions. NSA's surveillance of SWIFT, in particular, violates a 2010 agreement with the European Union. One GCHQ document quoted by Der Spiegel says the financial data it collects on behalf of the NSA contains "rich personal information" and that "a lot of it is not about our targets."

Minaret monitored the overseas communications of anti-war activists, civil rights leaders and even two sitting U.S. senators between 1967 and 1973. Targets included Martin Luther King Jr., Muhammad Ali, Jane Fonda, Stokely Carmichael, Sen. Frank Church (D-Idaho) and Sen. Howard Baker (R-Tenn.). The New York Times's Washington bureau chief, Tom Wicker, and Washington Post columnist Art Buchwald were also targeted.

LOVEINT In response to a request from Sen. Charles Grassley (R-Iowa), the NSA's Office of the Inspector General releases details of the 12 "substantiated instances" of "intentional and willful" misuse of NSA surveillance authority since January 2003. Most involved so-called "love intelligence" where agents spied on current or former love interests. The incidents were discovered through agency audits and self-reports.

NSA Attacks TOR. NSA and GCHQ's attempts to compromise the TOR network - a web browser that allows users to conceal their identities. The Guardian reports that intelligence agencies used a vulnerability in an older version of Mozilla's Firefox web browser to implant surveillance software on some TOR users' computers when they visited specific websites.

NSA and Encryption. NSA has cracked methods of encryption used by millions of people ever day for secure email, e-commerce, financial transactions and more. According to these reports, the NSA maintains a database of common decryption keys - some possibly stolen from private companies. Also, NSA collaborates with the tech industry to implant security back doors into consumer products; the U.S. works to weaken international encryption standards; and the British spy agency GCHQ implanted covert agents in technology companies.

Electronic Frontier Foundation Defending your rights in the digital world

EFF Files Brief to Reveal the DEA's Secret Use of Electronic Surveillance in Criminal Cases October 15, 2013 | By Hanni Fakhoury

Given the recent revelations about just how pervasive the government's electronic surveillance has been, it's no surprise these surveillance programs are popping up in criminal cases, as defense attorneys are finding gaps in how the government collected particular pieces of electronic evidence on their clients. A new amicus brief we filed today with the ACLU and the ACLU of Northern California in a drug case in San Francisco federal district court asks the court to order the government to fill these gaps.

The case involves 20 co-defendants charged with transporting and distributing drugs from San Francisco to Seattle. During the investigation, the government obtained records on over 700,000 phone calls made by more than 600 different phone numbers, including records such as numbers dialed or dialing in, the date, time and duration of the calls, and in some cases location information. Yet despite the sheer volume of calls at issue, the government produced to the defense attorneys court orders authorizing collection on only 52 of these phone numbers. The enormous discrepancy between the call data actually collected and the court orders authorizing the collection raises serious questions about whether the government took advantage of the controversial surveillance programs recently leaked to the press.

In June, details of the NSA's bulk telephone records collection program was published by The Guardian. **Then in August, Reuters reported about the NSA's practice of funneling information to the Drug Enforcement Administration's Special Operations Division ("SOD"). In turn, the DEA and SOD would use the information to generate its own independent leads and then deliberately omit the NSA's involvement in reports and affidavits, effectively "laundering" the intelligence.** Then, in September, the New York Times reported that DEA agents had direct access into AT&T's database known as "Hemisphere" that contained millions of records about phone calls dating back to **1987.** Like SOD, agents are deliberately instructed to omit referencing the Hemisphere program in court documents.

With all this information coming to light, criminal defendants are fighting to uncover what type of electronic surveillance really occurred in their criminal cases, and how information was obtained by the government. In our amicus brief, we ask a federal district court to order the government to provide more information about how it potentially used these surveillance programs in criminal cases.

For example, investigators in the San Francisco drug case were able to locate a phone number for a suspect only two days after his prior number had been disconnected. The reports turned over to defense attorneys indicated that the information was obtained by a confidential source, and that may very well be true. But this ability to connect an old phone number with a new one sounds exactly like what the **Hemisphere** program is capable of doing. Yet, there's no mention of the Hemisphere program in any of the investigative reports, a glaring omission that is consistent with

the DEA's directive to agents to "never refer to Hemisphere in any official document" and instead lie that the "results were obtained from an AT&T subpoena."

Deliberately omitting this information is all part of DEA's act of, in their own words, "protecting the program." As we explain in our amicus brief, this deliberate omission runs afoul of the Fifth Amendment's guarantee of due process. Specifically, under Brady v. Maryland, the government must disclose "material" evidence that is favorable to the defense. "Material" means the evidence could affect the outcome of the criminal proceeding and Brady's obligation extends to "material" facts relevant to raising Fourth Amendment challenges. Here, understanding if and how these surveillance programs were used would be "material" for three reasons.

First, if these programs were used to obtain evidence against a criminal defendant, the defendant must be given an opportunity to challenge that evidence. They couldn't do so without the full facts of whether the programs were used, and how. Second, the government must turn over evidence that bears on the credibility of a witness. A witness' credibility is an important factor in determining whether probable cause exists, and that obligation is not just reserved to the government's use of human witnesses. The Ninth Circuit Court of Appeals (which has jurisdiction on the federal court in San Francisco) has explained that these discovery obligations require the government to disclose evidence of a drug detecting dog's reliability. We believe the same obligations extend to electronic surveillance too. Third, in Franks v. Delaware, the US Supreme Court ruled that a criminal defendant has a right to challenge false or deliberately omitted statements in a search warrant affidavit. In turn, the Ninth Circuit has held Brady requires prosecutors to disclose evidence that could be used to impeach the testimony of an officer at a suppression hearing. Thus, to the extent officers used the program, it would impeach their claims that they relied on an administrative subpoena or a confidential source to get the information.[17]

While it may seem like connecting these surveillance programs to domestic criminal cases is "highly hypothetical," the operation of these programs outside of the public eye, coupled with the directive that agents utilizing SOD and Hemisphere hide the existence of the programs from even judges and prosecutors means courts must require the government to dig deeper and untangle how electronic surveillance actually occurred in a criminal case. The Supreme Court in Franks noted the Fourth Amendment "would be reduced to a nullity if a police officer was able to use deliberately falsified allegations to demonstrate probable cause, and, having misled the

---

[17] U.S. v. Barton (9th Cir. 1993) 995 F.2d 931, 935 (where the defendant alleged the government agents destroyed evidence necessary to impeach allegations in a search warrant affidavit, the appellate court held "that the due process principle announced in Brady and its progeny must be applied to a suppression hearing involving a challenge to the truthfulness of allegations in an affidavit for a search warrant"); *accord* Smith v. Black (5th Cir. 1990) 904 F.2d 950, 965-66, vacated on other grounds, 503 U.S. 930 (1992); *see* discussion in U.S. v. Stott, 245 F.3d 890, 902 (7th Cir. 2001). *Cf.*, Magallan v. Superior Court (People) (2011) 192 Cal.App.4th 1444 (defense has a right to pre-preliminary discovery to prove a Fourth Amendment violation.)

magistrate, then was able to remain confident that the ploy was worthwhile." We hope the Court here and in other criminal cases orders the government to come clean.

https://www.eff.org/deeplinks/2013/10/new-amicus-brief-urges-court-order-criminal-discovery-surveillance-programs