BNA

The "Ins" and "Outs of Electronic Information Criminal Investigations and Actions

March 10, 2011

"REPRESENTATIVE" DECISIONS

FEDERAL DECISIONS

***Application for Warrant for E-Mail Account,* Mag. No. 10-291-M-01 (D.D.C. Nov. I, 2010). A magistrate judge had ordered the Government to notify the subscriber or customer of an e-mail account that a warrant had been issued for its contents. Interpreting the Electronic Communications Privacy Act, the district court reversed. The district court held that the ECPA incorporated the procedural provisions of *Fed. R. Crim. P.* 41 and that the**

rule was satisfied by serving the warrant on the ISP provider.

WORDS AND PHRASES: ELECTRONIC COMMUNICATIONS PRIVACY ACT, SEARCH WARRANT, FED. R. CRIM. P. 41

***Doe v. Shurtleff,* 2010 WL 4888036 (10th Cir. Dec. 1, 2010). In this action, the anonymous plaintiff had been convicted of sex offenses involving a minor in a United States military court. The plaintiff challenged in the District Court a Utah statute that required him, as a resident and convicted sex offender, to provide to the Utah Department of Corrections, among other things, all "Internet identifiers." After the District Court found that the statute had no restrictions on the dissemination of information and held it unconstitutional as an infringement of the plaintiff's First Amendment right to anonymous speech, Utah amended the statute. The District Court then granted a Rule 60(b) motion and upheld the statute. On appeal, the Court of Appeals affirmed (and denied a motion for panel rehearing and rehearing *en banc*). The Court of Appeals concluded, among other things, that the amended statute was "content-neutral" and did *not* require strict scrutiny, that the statute did *not* allow unrestricted dissemination to the general public, and that the plaintiff did not have a reasonable expectation of privacy in his "online identifiers."**

WORDS AND PHRASES: FIRST AMENDMENT, REASONABLE EXPECTATION OF PRIVACY

***In re Application,* 2010 WL 5437209 (E.D.N.Y. Dec. 23, 2010). At issue here was whether the Government was required to obtain a search warrant for the disclosure of "historical cell-site information" over a period of 113 days. The Government had sought to proceed by order under Section 2703(d) of the Stored Communications Act. In holding that a warrant was required with a showing of probable cause, the magistrate judge rejected as binding an *order* by a district judge which reversed a similar ruling he had made. Instead, the magistrate judge relied on other decisions, including *United States v. Maynard,* and concluded that a subscriber had a reasonable expectation of privacy in "the most sensitive information about a person's life—information that goes far beyond the ordinary course of the service provider's business."**

WORDS AND PHRASES: FOURTH AMENDMENT, REASONABLE EXPECTATION OF PRIVACY, SEARCH WARRANT, STORED COMMUNICATIONS ACT

***In re Application for Search Warrant,* Mag. No. 09-320 (D.D.C. June 6, 2009). Here, the court denied the Government's**

request for reconsideration. The court had refused to authorize the search of electronic devices. In denying the request, the court affirmed that mere references to use of a computer are insufficient: "Without proof of a consistent use of the computer to communicate or otherwise advance of the conspiratorial scheme, it cannot be said that the computer is being used as an instrumentality of a crime." The court also denied reconsideration of its refusal to allow a search for foreign language documents: "Many Americans (including me) grew up in bilingual homes. That alone cannot be justification to search those homes for documents in a foreign language."

WORDS AND PHRASES: SEARCH WARRANT, GENERAL SEARCH

***In re Boucher,* 2009 WL 424718 (D. Vt. Feb. 19, 2009). A magistrate judge had quashed a grand jury subpoena on the grounds that it violated the defendant's Fifth Amendment right against self-incrimination. In reversing the magistrate judge, the court held that requiring the defendant to produce an unencrypted version of a laptop drive would not be a "compelled testimonial communication" as the Government was already aware of the existence and location of the drive and its contents (child pornography). However, the court did bar the Government from using the production to authenticate the drive or the contents.**

WORDS AND PHRASES: GRAND JURY SUBPOENA, FIFTH AMENDMENT PRIVILEGE AGAINST SELF-INCRIMINATION, AUTHENTICATION

In re: Grand Jury Subpoenas, **No. 10-15758 (9th Cir. Dec. 7, 2010). Here, the United States appealed from an order quashing subpoenas on the respondent law firms. The subpoenas, issued under Fed. R. Crim. P. 17(c), sought nonprivileged materials in aid of a grand jury investigation of the firms' clients. The materials had been obtained by the firms through discovery in a private antitrust action. The Court of Appeals reversed, holding that the District Court had abused its discretion. There was no proof of "collusion between the civil suitors and the government" and the Government had not engaged in any bad faith tactics. "By a chance of litigation, the documents [in issue] had been moved from outside the grasp of the grand jury to within its grasp. No authority forbids the government from closing its grip on what lies within the jurisdiction of the grand jury."**

WORDS AND PHRASES: GRAND JURY SUBPOENA

In the Matter of the Search of Motorola Cellular Telephone, **Mag. Nos. 09-m-652 through 09-653 (D.D.C. Dec. 7, 2009). The**

Government sought the issuance of search warrants for two seized cell phones. Noting the ability of cell phones to hold vast amounts of data, that the supporting applications did not specify what information the Government sought, and that no limitations on the searches were proposed, the court found that a "general search" was being requested. The court denied the application.

WORDS AND PHRASES: SEARCH WARRANT, GENERAL SEARCH

***In re Subpoenas,* 2010 WL 841258 (W.D. Va. Mar. 10, 2010). The Government served two investigative subpoenas on Abbott Laboratories "for a number of potential federal violations arising out of Abbott's impermissible off-label marketing" of a drug and for related health care fraud. After Abbott argued that the subpoenas were unduly burdensome, the Government offered to narrow the scope of the subpoenas to seek email from three people. In granting the Government's motion to compel compliance with the subpoenas as modified (which required Abbott to produce "live" e-mail and "snapshots" from backup tapes over a specific time period), the court found the subpoenas to be "reasonable" under the Fourth Amendment: The email sought was relevant to the investigation. The email was on backup tapes preserved for other litigation and Abbott had nearly $30**

billion in annual sales. Moreover, "if retrieving the e-mails the government requests is as difficult as Abbott conveys, then the fault lies not so much with an overly broad governmental request as it does with Abbott's policy or practice of retaining documents (documents Abbott has been required to retain for litigation purposes) in a format that shrouds them in practical obscurity." The court also rejected Abbott's argument that it was unduly burdensome "to formulate search terms relating to the off-label marketing of other FDA approved drugs."

WORDS AND PHRASES: FOURTH AMENDMENT, SUBPOENA

***In re: TFT-LCD (Flat Panel) Antitrust Litigation,* 2009 WL 2905898 (N.D. Ca. Sept. 10, 2009). In this rare sojourn into the world of grand jury subpoenas, a corporation sought to compel the Department of Justice to return an inadvertently produced document included on a hard drive turned over in response to a subpoena. The document contained an employee's notes about an FBI interview and had been prepared at counsel's direction. Citing Federal Rule of Evidence 502(b), the court found that reasonable steps (unknown from the opinion) had been taken to prevent and rectify the disclosure, although the document had been in DOJ's possession for over 22 months and DOJ had used it to prepare its case. The court declined to address "any collateral**

consequences" of the disclosure and noted DOJ's concern that parties might insert "Trojan Horses" into a production to secure some type of immunity from prosecution.

WORDS AND PHRASES: GRAND JURY SUBPOENA, FED. R. EVID. 502(b), INADVERTENT PRODUCTION, WAIVER OF PRIVILEGE

***United States v. Ahrndt,* 2010 WL 373994 (D. Ore. Jan. 28, 2010). The defendant, a previously-convicted sex offender, was charged with transportation and possession of child pornography. He moved to suppress evidence derived from his use of a wireless network to connect with the Internet. A neighbor using the same network accessed shared files of the defendant indicative of child pornography and notified the police who, with the neighbor, observed child pornography. The police identified the defendant as a registered sex offender, accessed the network and determined its IP address after securing a search warrant, served a summons on Comcast and learned that the defendant was the subscriber for the IP address, and then secured a second warrant for media containing child pornography at the defendant's home. The defendant argued that the police violated the Fourth Amendment when the police initially accessed the defendant's files through the neighbor's computer. The court held that the defendant had a lower expectation of privacy in**

information broadcast over an unsecured wireless network than through a hardwired or password-protected one and that the defendant had no reasonable expectation of privacy in the file-sharing program in issue (iTunes). The court also rejected the defendant's argument that the neighbor and the police had violated the Electronic Communications Privacy Act when they accessed his network because his network was "readily accessible to the general public." Finally, the court found that the defendant had no subjective expectation of privacy: He was a "somewhat sophisticated computer user" and should have known about shared files and the unsecured nature of his network even if he did not know these facts.

WORDS AND PHRASES: WARRANTLESS SEARCH, REASONABLE EXPECTATION OF PRIVACY, ELECTRONIC COMMUNICATIONS PRIVACY ACT

***United States v. Banks,* 556 F.3d 967 (9th Cir. 2009). In this pre-*CDT* decision, the Court of Appeals affirmed the defendant's conviction for child pornography-related offenses. The defendant argued, among other things, that the district court had erred in denying his motion to suppress evidence seized pursuant to a search warrant. The court held that the supporting affidavit established an adequate foundation for issuance of the warrant. There was sufficient**

information that the defendant was engaged in the transmission of images of minors engaged in sexually explicit conduct and expert opinion was not necessary to show how "pedophiles act in the digital age." The court also held that the warrant, which did not exclude the defendant's home-based business from any search, could not have been more specific given the nature of computer systems.

WORDS AND PHRASES: FOURTH AMENDMENT, SEARCH WARRANT, SCOPE OF SEARCH

***United States v. Beckett,* 2010 WL 776049 (11th Cir. Mar. 9, 2010) (*per curiam*). The defendant created a fake MySpace account that appeared to belong to an underage girl and used it to contact underage boys through MySpace and Instant Messaging. He would then coerce the boys into engaging in sexual acts. After being convicted of various crimes arising out of the "scam," the defendant appealed, arguing that the trial court should have suppressed subscriber information received by law enforcement in response to "exigent circumstances" letters sent to Internet Service Providers and phone companies ("providers"). Based on the information, a warrant was secured, the defendant's computers and related media were seized, and he was arrested. A computer search revealed "a plethora of child pornography and evidence connecting the**

computer to conversations" with the boys. The defendant argued on appeal that no "emergency" existed under the Electronic Communications Privacy Act which justified the disclosure of subscriber information in response to mere letters. In affirming the defendant's conviction, the Court of Appeals held that the ECPA does not provide a statutory suppression remedy absent a constitutional violation. There was no Fourth Amendment violation, as the defendant had no reasonable expectation of privacy in "identifying information transmitted during internet usage and phone calls that is necessary for the … [providers] to perform their services" (as opposed to content)—and that the defendant had entered into written agreements with the providers that prohibited use of services for illegal activities and that allowed the providers to turn over subscriber information related to such activities. The court also rejected the defendant's argument that law enforcement exceeded the scope of the warrant when the content of his computers were searched.

WORDS AND PHRASES: ELECTRONIC COMMUNICATIONS PRIVACY ACT, SEARCH WARRANT, SCOPE OF WARRANT

***United States v. Borowy,* 2010 WL 537501 (9th Cir. Feb. 17, 2010) (*per curiam*). The defendant entered a conditional plea to possession of child pornography and appealed from the**

denial of his motion to suppress evidence. (He also appealed from a Rule 11 error). An FBI agent had conducted a keyword search on a publicly available peer-to-peer file-sharing network and, using a software program, identified images of child pornography. The agent then downloaded and viewed files from the defendant's IP address, several of which contained child pornography. The agent then secured a search warrant and seized the defendant's laptop, CDs, and floppy disks. Forensic examination revealed hundreds of child pornographic images. The court of appeals affirmed, holding that the defendant had no expectation of privacy in a file-sharing network. The court also held that the defendant's "ineffectual effort" to prevent the sharing of his files did *not* create an objectively reasonable expectation of privacy. The court rejected the defendant's argument that the agent's use of the software program constituted an unlawful search, as the contents of the defendant's files were already available to the public. Finally, the court held that the agent had probable cause to download files. The court did not resolve "whether downloading a file constitutes a seizure." The court also noted that it was only presented "with the limited case of a targeted search of publicly exposed information for known items of contraband" and rejected the defendant's argument that its decision would "allow unrestricted government access to all internet communications."

WORDS AND PHRASES: REASONABLE EXPECTATION OF PRIVACY, PROBABLE CAUSE

***United States v. Burgess,* 576 F.3d 1078 (10th Cir. 2009). The defendant appealed from the denial of his motion to suppress evidence of possession of child pornography. The evidence was on a laptop and two hard drives seized during the warrantless search of his motor home after a traffic stop and canine alert and searched thereafter pursuant to a warrant. In affirming, the Court of Appeals declined to adopt the Government's argument that the media could be searched under the "automobile exception" to the Fourth Amendment warrant requirement. It did question in *dicta,* however, whether the Supreme Court would treat computers differently from traditional "closed containers" because of the storage capacity of the former. Decided shortly before *United States v. Comprehensive Drug Testing, Inc.*, the Court of Appeals also stated: "It is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives."**

WORDS AND PHRASES: WARRANTLESS SEARCH

***United States v. Bynum,* 2010 WL 1817763 (4th Cir. May 5, 2010). The defendant appealed from his conviction for transportation and possession of child pornography. The defendant had been identified after an agent entered a "child-pornography online chat group administered" by Yahoo and observed an unknown person uploading photos. The Government served an administrative subpoena on Yahoo, which provided subscriber information and IP addresses. The Government located the associated ISP, which provided an email address and telephone number in response to a subpoena. The Government secured the defendant's name and address from the "subscriber information." Then, and after again observing the person in the chat group, the Government secured a search warrant for the defendant's residence, seized his laptop, and found child pornographic images. On appeal, the defendant argued that he had a reasonable expectation of privacy in the subscriber information secured through the subpoenas. The Court of Appeals disagreed. The defendant "voluntarily conveyed all this information to his internet and phone companies" and had no subjective expectation of privacy. Moreover, even if he did, "such an expectation would not be objectively reasonable." The appellate court also rejected, among other things, the defendant's argument that minor errors in the**

affidavit supporting the search warrant negated probable cause.

WORDS AND PHRASES: PROBABLE CAUSE, REASONABLE EXPECTATION OF PRIVACY, SEARCH WARRANT

***United States v. Christie,* No. 09-2908 (3d Cir. July 16, 2010). On this appeal from his conviction for various child pornography-related offenses, the defendant challenged, among other things, the admissibility of two posts he had made on a web site. In rejecting the challenge, the Court of Appeals held that the posts (which the defendant admitted he had made) were relevant and that, although the posts were "no doubt prejudicial," the district court had not abused its discretion in admitting the posts. The Court of Appeals also held that the district court had not erred in denying a motion to suppress: "no reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including ISPs."**

WORDS AND PHRASES: ADMISSIBILITY, REASONABLE EXPECTATION OF PRIVACY, SEARCH WARRANT

***United States v. Cioffi,* 2009 WL 3416241 (E.D.N.Y. Oct. 26, 2009), *opinion amended and superseded by U.S. v. Cioffi,* 668**

F. Supp. 2d 385 (E.D.N.Y. 2009). Ruling on the defendant's motion to suppress evidence seized from his personal email account pursuant to a search warrant, which had been served and responded to by Google, the court found that the application used to establish probable cause had not been attached or incorporated into the warrant and that the warrant did not limit any emails to be seized to those evidencing crimes. The court found that the defendant had a reasonable expectation of privacy in his personal email account. The court noted heightened concerns over the need for specificity when searching electronic information and considered several approaches to address those concerns, including that taken in *United States v. Comprehensive Drug Testing, Inc.* Rejecting the presearch protocol approach of *CDT,* the court granted the motion as the warrant lacked specificity. The court also rejected the Government's argument s that the "good faith' and "inevitable discovery" exceptions applied.

WORDS AND PHRASES: SEARCH WARRANT, PARTICULARITY, GOOD FAITH EXCEPTION, INEVITABLE DISCOVERY, REFERENCE TO *CDT*

***United States v. Comprehensive Drug Testing, Inc.,* 579 F.3d 989 (9th Cir. Aug. 26, 2009) (*en banc*). In what is fair to say is a**

controversial ruling stemming from grand jury investigations of steroid use by baseball players, the Court of Appeals set forth detailed protocols on how the Government and magistrate judges should proceed with search warrant applications where electronic information will be sought. These include Government waiver of reliance on the plain view doctrine, use of taint teams or third parties to segregate and redact information, disclosure of the risk of destruction of information seized, use of a search protocol tailored to locate only information for which probable cause exists and examination of such information only by case agents, and destruction or return of nonresponsive information.

NOTE THAT A REVISED OPINION WAS ISSUED ON SEPTEMBER 13, 2010: *United States v. Comprehensive Drug Testing, Inc.,* No. 05-10067 (9th Cir. Sept. 13, 2010)(*en banc*). In this, the Court of Appeals "dropped" the protocols described above and, in a concurring opinion, three judges referred to the protocols as "guidance" that "offers the government a safe harbor, while protecting the people's right to privacy and property in their papers and effects."

WORDS AND PHRASES: SEARCH WARRANT, GENERAL SEARCH, PLAIN VIEW

United States v. Dobbs, **No. 09-5025 (10th Cir. Jan. 5, 2011). The defendant had been convicted of the knowing receipt of two images of child pornography found on the hard drive of his computer. The images had been found on the hard drive's temporary Internet files folder, or "cache." The Court of Appeals reversed. The court noted that a cache can be populated with images "regardless of whether they are displayed on the computer's monitor" and that "a user does not necessarily have to see an image for it to be captured by the computer's automatic-caching function." Absent evidence that the defendant had accessed the cached images or that he was aware of his computer's caching function, there was insufficient evidence that he had "knowingly" received the images. [NOTE THAT THE STATUTE UNDER WHICH THE DEFENDANT WAS CHARGED HAS BEEN AMENDED TO PROSCRIBE "KNOWINGLY ACCESSING SEXUALLY EXPLICIT IMAGES WITH THE INTENT TO VIEW THEM"].**

WORDS AND PHRASES: SCIENTER

United States v. Drew, **259 F.R.D. 449 (C.D. Cal. 2009). In this matter of first impression arising out of postings on a website by the defendant and others that led to a minor's suicide, the court held that the intentional breach of an Internet website's terms of service could not survive a constitutional**

"vagueness" challenge and be punished under a provision of the Computer Fraud and Abuse Act.

WORDS AND PHRASES: COMPUTER FRAUD AND ABUSE ACT

***United States v. Durdley,* 2010 WL 916107 (N.D. Fla. Mar. 11, 2010). The defendant was indicted for distribution and possession of child pornography. He moved to suppress evidence seized pursuant to a search warrant. The defendant was employed by a public entity as a paramedic. While working, he accessed a computer owned by the entity. When the defendant left, he left a thumb drive in the computer. A supervisor opened the thumb drive and related ESI. A police officer arrived and conducted a warrantless search and seizure of the thumb drive. After an interview, the defendant was arrested, a State search warrant was issued, and hardware and software was seized from the defendant's residence. In denying the motion to supress, the court found that the defendant had inadvertently shared his ESI with the users of the public computer and that the supervisor had not acted as a law enforcement officer in accessing the ESI. Moreover, the warrantless search by the officer did not exceed that of the supervisor. Thus, he had no reasonable expectation of privacy. The court also held that the inclusion of erroneous**

information in the search warrant did not negate probable cause.

WORDS AND PHRASES: PROBABLE CAUSE, REASONABLE EXPECTATION OF PRIVACY, SEARCH WARRANT

***United States v. Farlow,* 2009 WL 4728690 (D. Me. Dec. 3, 2009). Here, the court declined to suppress evidence of child pornography seized from a computer pursuant to a search warrant. Before the warrant had issued, the defendant had been communicating with a minor (actually a New York City police officer) over the Internet while speaking with a police officer in Maine, who secured a first warrant during the communications. A second warrant followed the search of the defendant's computer when Maine was searching for non-pornographic images and came upon child pornography. Rejecting the defendant's reliance on *Comprehensive Drug Testing,* ("Even the most computer literate of judges would struggle to know what protocol is appropriate in any individual case . . . ."), the court denied the motion. The warrant was not overbroad but was limited in scope to evidence of crimes under investigation and the plain view doctrine applied.**

WORDS AND PHRASES: SEARCH WARRANT, OVERBREDTH, PLAIN VIEW, REFERENCE TO *CDT*

***United States v. Frenchette,* 583 F.3d 374 (6th Cir. 2009). In this appeal from an order suppressing evidence seized pursuant to a search warrant, the defendant had paid for a one-month subscription to a child pornography web site, but the district court found that the subscription was over a year old and "stale," thus not supporting probable cause. In reversing, the court of appeals held that the supporting affidavit demonstrated the likely continued presence of child pornography on the defendant's computer despite the passage of time and the presence of the defendant at an address identified with the subscription.**

WORDS AND PHRASES: SEARCH WARRANT, PROBABLE CAUSE

***United States v. Graham,* 2008 WL 2098044 (S. D. Ohio May 16, 2008). The defendants, indicted for tax violations, moved to dismiss the indictment on Speedy Trial Act grounds. Voluminous electronic information had been produced by the Government on a rolling basis. The information was tainted and incomplete. Defense counsel had been unable to manage review of that information. No trial date was in sight. For all these reasons, and faulting the Government, defense counsel, and itself, the court dismissed the indictment without prejudice.**

WORDS AND PHRASES: SPEEDY TRIAL ACT

***United States v. Heckman,* 592 F.3d 400 (3d Cir. 2010). The Court of Appeals reversed the imposition of special conditions on a convicted child pornographer, included one that imposed an unconditional lifetime ban on Internet access by the defendant. Distinguishing *United States v. Thielemann,* the court noted that the defendant's conviction involved the "transmission of child pornography rather than the direct exploitation of children." Regardless of whether the defendant was a "serial offender" (which he was), there were other less restrictive conditions, which could control his behavior.**

WORDS AND PHRASES: SPECIAL CONDITIONS

***United States v. Hill*, 2011 WL 90130 (N.D. Cal. Jan. 10, 2011). After a young girl reported that a man in a white SUV exposed himself to her, and after she subsequently identified him, the Marin Sheriff's Deputy arrested the man, confiscated his iPhone, and searched the phone immediately and again when they returned to the station, all without a warrant. Upheld the search at the scene as a valid search incident to arrest, analogizing the iPhone to an element of the Defendant's clothing or a wallet taken from his person, and further upheld the subsequent search at the station because the iPhone remained in the continued and uninterrupted possession of**

law enforcement. Suppressed warrantless inventory search of separate iPod seized from impounded car six days later for failure to comply with standard inventory procedures.

WORDS AND PHRASES: FOURTH AMENDMENT, WARRANTLESS SEARCH

***United States v. Kilbride,* 584 F.3d 1240 (9th Cir. 2009). The defendants were convicted of various crimes (including several related to obscenity) arising out of their sending unsolicited bulk email ("spam") advertising adult websites. On appeal, they challenged, among other things, the jury instructions on "contemporary community standards." Rejecting this challenge, the court of appeals held that no precise geographic of the relevant community was required. The court also held that "a national community standard must be applied in regulating obscene speech on the Internet, including obscenity disseminated via email," but that, given the unsettled state of the law at the time, the trial court had not committed plain error by failing to give that charge.**

WORDS AND PHRASES: JURY INSTRUCTIONS

***United States v. King,* 2010 WL 1729733 (3d Cir. 2010). The defendant appealed from a sentence following a conditional**

guilty plea to interstate transportation to engage in sex with a minor (and under truly reprehensible facts). Law enforcement had gained entry to the defendant's residence with an arrest warrant for another resident. When that resident was arrested, she consented to the seizure of her computer. The defendant objected, contending that the hard drive belonged to him. The district court denied a motion to suppress evidence secured after this initial seizure. As stated by the Court of Appeals, "[t]hese facts present a novel question of law: when an owner of a computer consents to its seizure, does that consent include the computer's hard drive even when it was installed by another who claims ownership to it and objects to its seizure." Answering "yes," the court held that a computer was a "personal effect," and that the defendant relinquished any privacy in the hard drive when he placed it in a computer shared with another.

WORDS AND PHRASES: FOURTH AMENDMENT, REASONABLE EXPECTATION OF PRIVACY

***United States v. Koch,* No. 10-1789 (8th Cir. Nov. 17, 2010). During a valid search of the defendant's apartment for evidence of illegal gambling activities, law enforcement seized a Compaq computer and flash drive. After the defendant pled guilty to a gambling offense, law enforcement prepared to**

dispose of the seized items. An agent called a prosecutor for advice and then secured a disposal order from a State judge. Agents then viewed the contents of the drive and discovered images of child pornography. They then stopped the inspection, secured a search warrant for the computer, and discovered more images, after which the defendant was charged with possession. The district court denied a motion to suppress and found the defendant guilty after a bench trial. The Court of Appeals affirmed. The court concluded that the agents had acted in objective good faith in opening the drive. The Court of Appeals also, among other things, rejected the defendant's argument that there was insufficient evidence of knowing possession: There was evidence that the defendant had manipulated the images rather than that the images had been stored automatically in a cache. The court also affirmed a special condition that restricted his computer use and Internet access, noting that the defendant was a sophisticated computer user.

WORDS AND PHRASES: GOOD FAITH EXCEPTION, SEARCH WARRANT, SPECIAL CONDITIONS

***United States v. Ladeau,* 2010 WL 1427523 (D. Mass. Apr. 7, 2010). This criminal action began after the RCMP arrested a person who posted child pornography on an online network.**

Eventually, the Government secured the IP address for an another person who participated in the network and, through an administrative subpoena, identified the defendant, secured a search warrant, and seized child pornography. The defendant moved to suppress, arguing that he had a reasonable expectation of privacy because he used software intended to limit public access to the network. In denying the motion, the court found that the defendant had no *objective* expectation of privacy, as others could access the network and disseminate information about him. The court also found, among other things, that probable cause existed to seize evidence of child pornography in any form.

WORDS AND PHRASES: PROBABLE CAUSE, REASONABLE EXPECTATION OF PRIVACY, SEARCH WARRANT

United States v. Little,* No. 08-15964 (11th Cir. Feb. 10, 2010). The defendants produced and sold sexually explicit videos that were marketed online at sexually explicit websites. The defendants were convicted of obscenity-related offenses based on the trailers and on DVDs purchased through the websites. On appeal, the court of appeals rejected the defendants' argument (among others) that the "contemporary community standards" for defining obscenity was unconstitutional as applied to the Internet. Rejecting *United

States v. Kilbride, **the Eleventh Circuit held that the community standards of the trial court (the Middle District of Florida) applied.**

WORDS AND PHRASES: JURY INSTRUCTIONS

United States v. Mann, **592 F.3d 779 (7th Cir. 2010). Here, the defendant entered a conditional guilty plea of possession of child pornography and appealed the denial of his motion to suppress evidence of the pornography. The State of Indiana had secured a warrant to search for evidence of the crime of voyeurism (the defendant had installed a video camera in a women's locker room). Several months after the defendant's computers had been seized, an officer used, among other things, a "forensic tool kit" to search the computers and discovered child pornography on files "flagged" by the kit as containing child pornography. Several months thereafter, the officer searched another computer using the kit and found more child pornography. Accepting the district court's findings of fact that the officer was searching for evidence of voyeurism, the Court of Appeals rejected the appeal. Distinguishing precedent and relying in part on *United States v. Burgess*, the court held that the execution of the search was reasonable: "Undoubtedly the warrant's description serves as a limitation on what files may reasonably be searched. The**

problem with applying this principle to computer searches lies in the fact that such images [of women in locker rooms] could be nearly anywhere on the computers." The court rejected the argument that use of the kit was unreasonable *per se,* although the court held that the officer exceeded the scope of the warrant when he opened the flagged files. The court severed the evidence from those files. The court also rejected the defendant's reliance on *Comprehensive Drug Testing: "*we are inclined to find more common ground with the dissent's position that jettisoning the plain view doctrine entirely in digital evidence cases is an 'efficient but overbroad approach.' " The court was also "skeptical of a rule requiring officers to always obtain pre-approval from a magistrate judge to use the electronic tools necessary … ." Instead, the Court of Appeals cautioned those "involved in searches of digital media to exercise caution to ensure that warrants describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described." The court also found "troubling" the officer's failure to stop the search and apply for a new warrant when he uncovered evidence of child pornography. The court also expressed "distaste" for the timeline of the search.

WORDS AND PHRASES: SEARCH WARRANT, SCOPE OF WARRANT, PLAIN VIEW, REFERENCE TO *CDT*

United States v. Miller, **594 F.3d 172 (3d Cir. 2010). After the defendant was convicted of possession of child pornography, the trial court imposed a life term of supervised release as well as special conditions that, among other things, barred the defendant from accessing the Internet without prior approval and requiring him to submit to monitoring of his computer activities. Relying on, among other decisions, *United States v. Thielemann,* the Court of Appeals vacated, concluding that the lifetime restriction on access was excessive under the facts. On remand, the trial court was directed that any "new conditions of supervised release should integrate a more focused restriction on internet access with the requirement of computer monitoring into a comprehensive, reasonably tailored scheme."**

WORDS AND PHRASES: SPECIAL CONDITIONS

United States v. Ohle, **2011 WL 651849 (S.D.N.Y. Feb. 7, 2011). Here, citing *United States v. Skilling,* the district court rejected the defendants' claim that the Government had failed to fulfill its *Brady* obligations at trial because "materials were unduly onerous to access." The Government had produced several gigabytes of data — including million of separate files extending to several million pages in length — in nine separate databases, and any document search had to be**

conducted on a database-by-database basis. To facilitate review, defense counsel had been provided with an electronically searchable Concordance database. Both the Government and defense counsel had equal access to this database. Thus, the defendants were just as likely to uncover purportedly exculpatory evidence as the Government. Moreover, the court held that, as a general rule, the Government was under no duty to direct a defendant to exculpatory evidence within a larger mass of disclosed evidence.

WORDS AND PHRASES: *BRADY*

***United States v. O'Keefe,* 537 F. Supp. 2d 14 (D.D.C. 2008). Here, the court "borrowed" from the Federal Rules of Civil Procedure to address the adequacy of searches performed in discovery in a criminal proceeding and suggested that experts qualified under Fed. R. Evid. 702 would be required to testify about search methodology.**

WORDS AND PHRASES: DISCOVERY

***United States v. Pineda-Moreno,* 591 F.3d 121 (9th Cir. 2010). The Government installed mobile tracking devices on the defendant's vehicle while it was parked on a public street, in a**

public parking lot, and his driveway. The government used the information to track the defendant from a marijuana field. The defendant entered a conditional guilty plea to manufacturing marijuana after the district court denied his motion to suppress. On appeal, the defendant argued that his Fourth Amendment rights were violated. The court of appeals held that the defendant's vehicle was within the cartilage of his home when two devices were installed. However, since he took no steps to exclude the public from the driveway, the defendant had no reasonable expectation of privacy in it. The court also held that the defendant had no reasonable expectation of privacy when his vehicle was parked in public spaces. Finally, distinguishing *Kyllo v. United States* (which considered the use of thermal imaging technology to "search" with the cartilage of a home), the court rejected the argument that the use of "new" technology to track the location of the defendant's vehicle was a impermissible search. The court took note that several state supreme courts had reached the opposite conclusion under their respective State constitutions.

WORDS AND PHRASES: WARRANTLESS SEARCH, REASONABLE EXPECTATION OF PRIVACY

***United States v. Qadri,* 2010 WL 933752 (D. Hawaii Mar. 9, 2010). One defendant moved (a second time) to dismiss the indictment and superceding indictment for violation of the Speedy Trial Act. The defendant had been charged with, among other things, wire fraud. The indictments came nearly three years apart. ESI from over thirty hard drives and three servers was in issue. Although the Government did not respond to defense communications about production "expeditiously," the Government did produce a substantial number of documents and copied the hard drives for the defendant. There also appeared to be a problem with the defendant's ability to review the content of the servers. The defendant had consented to various continuances and had not established prejudice. The court denied the motion: "It appears that the delay in this case may be attributed at least in part to the nature of electronic discovery, the complex nature of the alleged crimes, and the necessity of coordinating various branches of government in the investigation." The court also denied the defendant's request for an evidentiary hearing.**

WORDS AND PHRASES: SPEEDY TRIAL ACT

***United States v. Raymond,* 2009 U.S. Dist. LEXIS (N.D. Okla. Sept. 16, 2009). In this child pornography prosecution, the**

court denied the defendant's request for access to images on a seized computer. The Government had mirror-imaged the hard drive and made the mirror image available to the defendant's expert. The expert contended that he could not locate all of the allegedly illegal images from among the 14.000 in total on the mirror image. The court held that the Adam Walsh Act superceded *Fed. R. Crim. P.* 16 and barred the Government from reproducing child pornography in response to a discovery request as long as materials were made "reasonably available" to a defendant. Here, the allegedly illegal images were made available for inspection by defense counsel. The court rejected the expert's suggestion that the mirror image had been stripped of metadata. The Government agreed to make available to the expert on CDs the "missing" images, although these remained in the possession of the Government. Finally, the court directed the parties to confer about Government production of redacted images for use by the defendant in subpoenaing information from Web site owners.

WORDS AND PHRASES: SUBPOENA, DISCOVERY

***United States v. Rodriguez,* 2010 WL 5253231 (11th Cir. Dec. 27, 2010). The defendant, a former Social Security Administration TeleService representative, accessed SSA**

databases for confidential information about women with whom he had relationships. He did so in violation of a SSA policy that prohibited obtaining information for nonbusiness reasons. The defendant was convicted of violating the Computer Fraud and Abuse Act. The Court of Appeals affirmed. The defendant had "exceeded" his authorized access. The Court of Appeals also rejected, among other things, the argument that the Act required proof that use of information be in furtherance of some crime. [NOTE: THERE MAY BE A SIGNIFICANT SPLIT BETWEEN THE CIRCUITS ON THE MEANING OF "WITHOUT AUTHORIZATION" AND "EXCEEDS AUTHORIZED ACCESS" UNDER THE ACT].

WORDS AND PHRASES: COMPUTER FRAUD AND ABUSE ACT

***United States v. SDI Future Health Inc*., 568 F.3d 684 (9th Cir. 2009). On this appeal from an order granting a motion to suppress evidence seized pursuant to a search warrant, the court of appeals addressed when employees have standing to challenge searches of corporate premises: "except in the case of a small, family-run business over which an individual exercises daily management and control, an individual challenging a search of workplace areas beyond his own internal office must generally show some personal connection to the places searched and the materials seized." The court of**

appeals remanded for further fact-finding. Turning to the corporation's challenge to the warrant, the court of appeals held that the warrant had incorporated the supporting affidavit by reference, that the affidavit "accompanied" the search, and that the warrant satisfied the particularity requirement. The court did, however, sustain the invalidity of the warrant on overbreadth grounds as to, among other things, email: There was no limitation placed on the email to be searched. The court also rejected the Government's reliance on "good faith" and held that the district court should have severed the unconstitutional portions of the warrant and allowed only partial suppression.

WORDS AND PHRASES: SEARCH WARRANT, PROBABLE CAUSE, OVERBROADNESS, GOOD FAITH, SEVERANCE

***United States v. Skilling,* 554 F.3d 529 (5th Cir. 2009). In this appeal from a conviction for, among other things, tax fraud, the defendant argued that the Government "dumped" an enormous volume of electronic information (several hundred million pages) on him in an attempt to conceal *Brady* material. The Government had provided the defendant with an "open file [that] was electronic and searchable." It also provided a list of "hot documents," created indices, and gave the defendant access to databases. Moreover, the case was**

complex and there was no evidence of wrongful conduct. Under these circumstances, the court held that the use of the open file did not violate *Brady.*

WORDS & PHRASES: *BRADY*

***United States v. Stabile*, 2011 WL 294036 (3rd Cir. Feb. 1, 2011). Upheld consent search (and subsequent seizure) of hard drives in search authorized by co-resident of house because computers were not password protected and were located in a common area. Upheld seizure (as opposed to mirroring on-site) given that co-resident did not limit scope of the search, evidence of crime could be found anywhere on hard drives, and practical considerations of investigating and seizing electronic evidence (including the length of time and the need for trained forensic investigators and a controlled environment for searches) made on-site collection of data impracticable. Waiting three months to obtain search warrant was not unreasonable delay in part because search was based on consent, not probable cause. Delay can render probable cause searches unreasonable, but consent searches involve a voluntary relinquishment of possession. Also, in balancing defendant's possessory interests in his computers against the government's rationale for the delay, the court noted that defendant waited 18 months to ask for his hard**

drives back, and the government's delay was attributable to an agent's assignment to a detail protecting the President and other high-level officials. Searches of hard drives were not unreasonable. First, it was permissible to "highlight" a suspicious folder called "Karzvid" (a reference to the peer-to-peer sharing program Kazaa that can be used to share music, movies, programs, and child pornography), thereby revealing file names and extensions that suggested child pornography, because (A) any suspicious folder can have evidence of any kind of crime (even though detective thought that folder might have child porn based on DVDs seized from the house with labels suggesting child pornography); (B) detective conducting search conducted a focused (as opposed to general) search to be sure his search complied with the search warrant procedures by physically inspecting the drive, making a copy to prevent damage or corruption, examining the file signatures to see if any were corrupted, conducting a hash value analysis to see if any files had been copied, and examining suspicious and out-of-place folders like the Kasvid folder; and (C) examining the file names was permissible under the plain view doctrine. Second, the court did not determine whether the detective's subsequent opening of 12 video files was justified under the plain view doctrine and instead applied the independent source doctrine based on the obtaining of a subsequent federal warrant that referenced

only the lurid file names (which provided probable cause) and not the content of the files. (The case also involved issues about naming the wrong hard drive in the federal warrant, and the court applied the inevitable discovery doctrine and did not suppress evidence).

WORDS AND PHRASES: FOURTH AMENDMENT, GOOD FAITH EXCEPTION, INEVITABLE DISCOVERY, PLAIN VIEW, REFERENCE TO *CDT,* SEARCH WARRANTS

***United States v. Stagliano,* 2010 WL 617364 (D.D.C. Feb. 19, 2010). The defendants were indicted for various obscenity-related offenses arising out of the use of an "interactive computer service." They challenged the statutes under which they were indicted on constitutional grounds. Rejecting the challenges, the court held, among other things, that the use of "community standards" did not render the statutes substantially overbroad. In so doing, the court declined to follow *United States v. Kilbride.* The court also rejected that the argument that the defendants had a right to "publish" (rather than merely possess) obscene materials.**

WORDS AND PHRASES: OVERBREDTH

***United States v. Suarez,* 2010 WL 4226524 (D.N.J. Oct. 21, 2010). Ruling on the defendants' motion to suppress or for an adverse inference instruction, the court found that the Government had failed to issue a litigation hold, as a result of which certain text messages between a cooperating witness and FBI agents had been deleted. The court also found that the deleted messages *could* have constituted Jencks Act material and should have been preserved. The court held that suppression of related evidence was unwarranted, as the Government had not acted in bad faith and there was no evidence that the deleted messages "clearly contained exculpatory material." The court did, however, agree to issue an adverse inference instruction and, to do so, "consult[ed] the more thoroughly developed civil case law on the subject." Applying a four-part test articulated in *Mosaid Tech. Inc. v. Samsung Elec. Co.,* 348 F. Supp.2d 332 (D.N.J. 2004), the court found that the Government had "control" over the messages, that there was "actual suppression or withholding" of the messages, that the deleted messages were relevant, and that it was reasonably foreseeable that the messages would be discoverable. The court also relied on *Pension Comm. v. Banc of America Sec.,* 685 F.Supp.2d 456 (S.D.N.Y. 2010), in framing the instruction.**

WORDS AND PHRASES: ADVERSE INFERENCE, "CONTROL," DUTY TO PRESERVE, JENCKS ACT, SCIENTER

United States v. Szymuszkiewicz, **No. 10-1347 (7th Cir. Sept. 9, 2010). The defendant had modified a "rule" on his supervisor's email account so that copies of email sent to her were automatically sent to the defendant. On an appeal from his conviction under the Wiretap Act, the Court of Appeals affirmed. First, the Court of Appeals rejected the defendant's argument that he should have been charged under the Stored Communications Act: "It is risky to defend against one crime by admitting another." The Court of Appeals then discussed the concept of "package switching" (by which email is routed from sender to recipient) and concluded that there had been an "interception" under the Wiretap Act. The Court of Appeals also held that the interception in issue was contemporaneous with the email, but rejected the incorporation of a "contemporanous" requirement into the Wiretap Act that had been adopted by other Courts of Appeals.**

WORDS AND PHRASES: STORED COMMUNICATIONS ACT, WIRETAP ACT

United States v. Thielemann, **575 F.3d 265 (3d Cir. 2009). Here, the Court of Appeals affirmed the imposition of special conditions on a convicted child pornographer. The conditions banned the defendant from possessing or viewing adult sexually explicit material and also restricted him from owning**

or operating a personal computer with Internet access anywhere without permission.

WORDS & PHRASES: SPECIAL CONDITIONS

***United States v. Voneida,* 337 Fed. Appx. 246 (3d Cir. 2009). The defendant was convicted of transmitting a threatening communication in interstate commerce after posting statements on his Myspace page. In affirming the conviction, the court of appeals rejected the defendant's argument that the statements had not been transmitted "because his postings were more like a hand-written diary." The court also rejected the argument that his postings were protected speech and that the prosecutor's reference to the Virginia Tech shootings (which happened several days before the postings) was *unduly* prejudicial.**

WORDS AND PHRASES: ???

***United States v. Vosburgh,* 2010 WL 1542340 (3d Cir. 2010). This was an appeal from a conviction for possession of child pornography. At its center was an "underground Internet message board." The board did not host child pornography but, instead, directed users to where child pornography could be found on the Internet. Access to the board was relatively**

difficult: "It is highly unlikely that an innocent user of the Internet would stumble across … [the site] through an unfortunate Google search." During a sting operation for users of the board, law enforcement came across an IP address that was traced to an ISP. In response to a subpoena, the ISP identified the defendant. When agents attempted to execute a search warrant at the defendant's residence, he destroyed various electronic media. Thereafter, agents secured a second warrant for a hard drive that they had inadvertently failed to seize the first time. "Thumbnail" images on the hard drive were introduced at trial. These images could not be accessed by the defendant. However, the Government argued that the thumbnails demonstrated that the defendant had possessed full-sized child pornographic images at some point. The Court of Appeals held that, given the unique nature of IP addresses, there was a fair probability that evidence of criminal activity would be found in the residence. The court also held that the application was not "stale," although there was a four month gap between it and attempts to access the site, observing that computers have long memories and that those interested in child pornography "tend to hoard their materials and retain them for a long time." The court also held that the Government's reliance on the thumbnail images did not constitute an impermissible amendment of the indictment and that there was sufficient evidence to support the

conviction (the defendant argued on appeal that his expert had "definitively disproved" the Government's case).

WORDS AND PHRASES: FOURTH AMENDMENT, SEARCH WARRANT, EXPERT

***United States v. Warshak,* 2010 WL 5071766 (6th Cir. Dec. 14, 2010). In this appeal from convictions arising out of a "massive scheme to defraud," the Court of Appeals held that a defendant had a reasonable expectation of privacy in the content of email held by an commercial Internet Service Provider (drawing an analogy to post offices and telephone companies) and that the Government violated the defendant's Fourth Amendment rights when it secured the email from the ISP by subpoena under Section 2703(b) and *ex parte* order under Section 2703(d) of the Stored Communications Act. However, the Court of Appeals concluded that an exclusionary remedy was inappropriate as the securing agents had relied in good faith on the constitutionality of the Act. The Court of Appeals observed, however, that "after today's decision, the good-faith calculus has changed, and a reasonable officer may no longer assume that the Constitution permits warrantless searches of private emails." The Government had failed to give the defendant notice of the subpoena or order, as required by Section**

2703(b)(1)(B). However, the Court of Appeals rejected the defendant's argument that this weighed against good faith, as the issue was reasonable reliance in *obtaining* the email. Likewise, the Court of Appeals rejected the defendant's argument that the Government's demand pursuant to Section 2703(f) that the ISP preserve his email *prospectively* violated the Act (although this was a subject of the concurrence). The Court of Appeals held, among other things, that the Government had acted properly in making large amounts of ESI available to the defendant. Rejecting the analogy to the Federal Rules of Civil Procedure made in *United States v. O'Keefe,* the Court of Appeals held that the Criminal Rules did not require the Government to produce ESI in a particular form, that much of the ESI was taken from computers that the defendants could access, that the defendants had an expert who could search the ESI, and the Government had given the defendants a "guide" to the ESI. The Court of Appeals also held that the Government had no obligation to "sift fastidiously" through the ESI to satisfy the Government's *Brady* obligations. Reviewing the counts on which the defendants were convicted, the Court of Appeals held, among other things, that there was sufficient evidence to conclude that a defendant had committed access-device fraud when he charged monies to customers' credit card accounts without consent. Although access to the monies in the accounts may

have been "ephemeral" (the monies were credited back immediately), the defendant did "receive" the monies and that was sufficient for conviction. The Court of Appeals did reverse the convictions under several counts and remanded for resentencing on others.

WORDS AND PHRASES: *BRADY*, DUTY TO PRESERVE, GOOD FAITH EXCEPTION, REASONABLE EXPECTATION OF PRIVACY, SEARCH WARRANT, STORED COMMUNICATIONS ACT

***United States v. Weaver,* 636 F. Supp. 2d 769 (C.D. Ill. 2009). Here, the Government moved to compel an ISP to comply with a subpoena and produce the contents of email sent or received by the defendant, accused of child pornography. Interpreting the Stored Communications Act, the court held that, for email less than 181 days old, an ISP must comply with a subpoena if email is "held or maintained solely to provide the customer storage of computer processing services." Disagreeing with a Ninth Circuit decision, and relying on a distinction between Web-bases and other email systems," the court also held Web-based email that is *opened* and then stored is not "in storage" under the Act. Under the facts *sub judice*, the court granted the motion.**

WORDS AND PHRASES: STORED COMMUNICATIONS ACT, SUBPOENA

United States v. Welch, **291 Fed. Appx. 193 (10th Cir. 2008). The defendant, convicted on child pornography charges, appealed the denial of motions to suppress evidence. The Government had begun drug investigations, which had "stalled" twice. In the interim, the Government learned that the defendant had operated a child pornography Website. The Government then secured a search warrant for rental premises owned by the defendant, located boxes containing drug-manufacturing materials, and made a warrantless arrest of the defendant. The Government then secured a search warrant for the defendant's residence to search for evidence of drug manufacturing. During execution of the warrant, the Government seized *non-networked* computer equipment. During a search of the electronic information on the seized items, the Government discovered child pornography on the unallocated space on a hard drive. The Government then secured a warrant to search for child pornography. The court of appeals held that there was no probable cause to believe that there was evidence of a drug crime at the rental premises, because, among other things, the supporting information was "stale." However, since all the known facts could have led to a reasonable belief that the evidence might be present and there was no police misconduct, the court applied the "good faith" exception. The court then rejected the defendant's argument that the second search warrant was**

overbroad: The warrant allowed computers to be searched for evidence of drug manufacturing, the Government could not identify what types of computer equipment it would encounter during the search, and the Government halted the search and applied for another warrant when it found child pornography. The court also rejected a "fruit of the poisonous tree argument."

WORDS AND PHRASES: SEARCH WARRANT, OVERBREDTH, GOOD FAITH

***United States v. Williams,* 592 F.3d 511 (4th Cir. 2010). The defendant was tried on stipulated facts and found guilty of possession of an unregistered machine gun, an unregistered silence, and child pornography. He appealed from the denial of his motion to suppress evidence. The State of Virginia had secured a warrant to search for and seize evidence of threats to bodily harm and harassment by computer. During execution of the search on various media, child pornography was found. The Court of Appeals rejected the defendant's argument that the scope of the warrant was exceeded: Evidence of child pornography was relevant to the offenses for which the warrant had been issued. Moreover, evidence of child pornography fell within the plain view doctrine as the warrant authorized the *search* of the media and the**

subsequent *seizure* of the contraband. The court also upheld the search of a lockbox containing the machine gum and the silencer, noting that the officers were entitled to inspect these items during their search for media that could have been inside the box.

WORDS AND PHRASES: SEARCH WARRANT, GENERAL SEARCH, PLAIN VIEW

***United States v. Wright,* 625 F.3d 583 (9th Cir. 2010). During an undercover search on a file-sharing program, an agent came across a user name in chat rooms. The agent downloaded a number of files, some of which contained child pornography. After a search warrant was executed at the defendant's apartment, he was convicted of transportation and possession of child pornography. The Court of Appeals, among other things, reversed the transportation conviction as there was no evidence that the files were transported "in interstate commerce" as the pornographic images in issue had not "travelled" outside one state (Arizona).**

WORDS AND PHRASES: INTERSTATE COMMERCE

***United States v. Yeley-Davis*, 2011 WL 167249 (10th Cir. Jan. 20, 2011). In methamphetamine distribution case, the court**

upheld the introduction at trial of certified telephone toll records containing information about phone calls made and received by defendant with other co-conspirators. The court rejected defendant's contention that the records violated her Sixth Amendment right to confrontation, holding that the evidence was not testimonial because Verizon kept the telephone records for business purposes and not solely for use at trial. Similarly, the authenticating custodial certifications were not testimonial because they were made to authenticate the records, not to prove or establish a fact at trial.

WORDS AND PHRASES: ADMISSIBILITY

STATE DECISIONS

DeVega v. State*, 2010 WL 337333 (Ga. Sup. Ct. Feb. 1, 2010). After being convicted of murder and other offenses, the defendant sought a new trial. He argued, among other things, that his trial attorney should have challenged on Fourth Amendment grounds the warrantless "ping" of his cell phone. The police used the phone to monitor the location of the phone from a public road, distinguishing *United States v. Karo

(which addressed the monitoring of a beeper from a private residence). The court found that the defendant had no reasonable expectation of privacy while traveling in public places.

WORDS AND PHRASES: WARRANTLESS SEARCH, REASONABLE EXPECTATION OF PRIVACY

***Gill v. State,* 300 S.W.3d 225 (Mo. 2010). The defendant, sentenced to death for first-degree murder, sought post-conviction relief, arguing that he was denied effective assistance of counsel. Trial counsel had been given a report about the contents of the murder victim's computer, which had been found in the defendant's car. The good character of the victim had been put in issue in the death penalty phase of the defendant's trial and, if counsel had investigated the computer, they would have found child pornography, with which they could have attacked the victim's character. Reserving the court below, the supreme court held that trial counsel's failure to investigate the contents constituted ineffective assistance of counsel and remanded for retrial of the penalty phase. The supreme court rejected a *Brady* challenge, noting that the report had been made available to trial counsel.**

WORDS AND PHRASES: *BRADY,* INEFFECTIVE ASSISTANCE OF COUNSEL

***In re Alex C.,* 2010 WL 5010391 (N.H. Sup. Ct. Nov. 30, 2010). The was an appeal from a trial court ruling that a delinquency petition was "true." The juvenile had sent twenty admittedly harassing instant messages to the mother of a girl who had run away. On appeal, the delinquent argued these were not "repeated communications" under New Hampshire law. The Supreme Court affirmed. The Court viewed IM , "not necessarily as some monolithic entity-a single conversation, but as a series of discrete electronic messages between two or more individuals."**

WORDS AND PHRASES: SUFFICIENCY OF EVIDENCE

***People v. Diaz,* S166600 (Ca. Sup. Ct. Jan. 3, 2011). The defendant challenged the fruits of the search of his cell phone. The defendant had been arrested after a controlled drug purchase and the phone seized incident to the arrest. Shortly after the arrest, the contents of the phone were searched and an incriminating message found. The defendant confessed after being confronted with the message. He moved to suppress, arguing that the warrantless search of the phone**

violated the Fourth Amendment. The motion was denied and the defendant pled guilty. The Court of Appeal affirmed. The California Supreme Court granted the defendant's petition for review. On the merits, and following "binding precedent" of the United States Supreme Court, the court held that the defendant's phone was "personal property" (not a "container") and that the warrantless search was valid, regardless of a delay in time. The majority rejected, over a vigorous dissent, the argument that the storage capacity of the phone was relevant and instead opted for a "bright-line" test.

WORDS AND PHRASES: FOURTH AMENDMENT WARRANTLESS SEARCH

***People v. J.J.*, 2010 WL 4033633 (Ca. Ct. App. Oct. 15, 2010). The juvenile in this proceeding had been made a ward of the court after being found to have illegally received a stolen motorcycle. He was placed on probation and a number of conditions imposed that he challenged on appeal. The Court of Appeal held that one condition, that barred the juvenile from any non-school-related use of computers, was unconstitutionally overbroad, as was a condition which barred him from the use of social media. The Court of Appeal also**

modified another condition so as to bar the juvenile from *knowing* use of a computer that was encypted or the like.

WORDS AND PHRASES: SPECIAL CONDITIONS

***People v. Kent,* 2010 WL 4008735 (N.Y. Sup. Ct. App. Div. Oct. 12, 2010). The defendant, a college professor, had been convicted of child pornography-related offenses after an employee of the college had run a virus scan on the defendant's office computer and found files of young girls, after which the college turned the hard drive over to police along with a "Consent to Search" form. In affirming the judgment of conviction, the Appellate Division addressed questions of first impression in New York. Among other things, the court held that "the mere existence of an image automatically stored in the cache, standing alone, is legally insufficient to prove either knowing procurement or knowing possession of child pornography." However, there was sufficient evidence to support the defendant's conviction. The court also rejected an ineffective assistance argument based on the failure of defense counsel to move to suppress the evidence collected from the hard drive. The defendant had no reasonable expectation of privacy in any personal files stored on his office computer because the computer was the**

property of the college and, therefore, there was a legitimate explanation for counsel's conduct.

WORDS AND PHRASES: INEFFECTIVE ASSISTANCE OF COUNSEL, SCIENTER

***People v. Klapper,* 2010 WL 1704796 (N.Y. Crim. Ct. Apr. 28, 2010). The defendant was charged with unauthorized use of a computer under New York law. The defendant was alleged to have installed keystroke-tracking software on a computer in his office and to have used that software to access the personal email account of an employee. On a motion to dismiss, the court held the allegations did not establish that the access was "without authorization." The defendant's ownership of, and authority over, the computer were of central importance. Moreover, the employee had a diminished expectation of privacy in the email communications. Absent allegations that the defendant had exceeded his right of access or that there was some restriction on that right, the motion was granted.**

WORDS AND PHRASES: COMPER FRAUD AND ABUSE ACT – STATE EQUIVILENT, REASONABLE EXPECTATION OF PRIVACY

People v. Nakai, **107 Cal. Rptr. 3d 402 (Ca. Ct. App. 2010). The defendant was found guilty under California law of attempting to send harmful material to a minor with intent to seduce. On appeal, the conviction was affirmed. Although the defendant wanted a Yahoo! dialogue with someone posing as a minor to be confidential, he had no reasonable expectation of privacy. Among other things, the defendant was on notice that dialogues might be shared in the investigation of illegal conduct and that others might have access to the dialogue.**

WORDS AND PHRASES: REASONABLE EXPECTATION OF PRIVACY

State v. Bailey, **2010 WL 724808 (Me. Sup. Jud. Ct. Mar. 4, 2010). After conviction of various child pornography-related offenses, the defendant appealed from the denial of his motion to suppress evidence. Police had been led to the defendant's apartment through their investigation of a peer-to-peer networking program. After a search of a nearby home, the police learned that someone was using an unsecured wireless router to access the network and disseminate child pornography. After turning off the router, a detective gained access to the apartment by telling the defendant that he was canvassing the neighborhood to see if anyone had a problem with computers being wrongfully accessed. The detective then**

gained access to the defendant's computer with the defendant's consent and searched it for files containing child pornography. The detective found, but did not open, the files. The defendant then acknowledged having a "problem" with child pornography and consented to a physical search, which yielded tapes that further implicated the defendant and adverse witnesses. On appeal, the Supreme Judicial Court reversed. The court concluded that the defendant had standing to challenge the search of his computer: He had a reasonable expectation of privacy in the computer and its contents when not being accessed through the network. Next, the court held that the defendant had consented to the initial search of the computer. Under the circumstances, the detective's deception was not such as to vitiate the consent. However, the detective exceeded the scope of the consent when "he ran a general search for *all* of the video files" (emphasis in original). Supressing the evidence secured through that search, the court remanded for consideration of an issue not on appeal: Whether other evidence should be suppressed as "the fruits of the poisonous tree."

WORDS AND PHRASES: WARRANTLESS SEARCH, REASONABLE EXPECTATION OF PRIVACY, SCOPE OF SEARCH

***State v. Barger,* 2011 WL 31786 (Ore. Sup. Ct. Jan. 6, 2011). Interpreting State law, the Oregon Supreme Court addressed whether a person could be found guilty of 'possess[ing] or control[ling]' digital images of sexually explicit conduct involving a child …, based on evidence showing only that the person searched for and found such images through the Internet" on his … computer." An officer had looked at the defendant's computer with his wife's consent and seen suspicious addresses on the computer's "web-address history." The computer was thereafter seized (again, with the wife's consent) and the hard drive imaged. After the drive was examined, the defendant was charged based on eight images found in the "temporary internet file cache." After a jury conviction, the defendant appealed, arguing that that there was insufficient evidence of possession or control. The Court of Appeals affirmed. The Oregon Supreme Court reversed, holding that "the acts here in issue—navigating to a website and bringing the images that the site contains to a computer screen—are not acts that the legislature intended to criminalize." The court noted that the defendant could have been charged under Oregon law with *viewing* child pornography if that act had been accompanied by some payment.**

WORDS AND PHRASES: SUFFICIENCY OF EVIDENCE

***State v. Carlson,* 778 N.W.2d 171 (Wisc. Ct. App. 2009) (*per curiam*). The defendant appealed from a conviction for possession of child pornography. Central to the trial was the defendant's allegation that he did not knowingly download the pornographic images but that, instead, he visited the Web sites accidentally or was involuntarily by a virus. The defendant argued on appeal that he was denied effective assistance of counsel because the computer expert selected by counsel was not "sufficiently knowledgeable." The court rejected the argument: "Counsel did not perform deficiently simply because the expert she located did not provide as much helpful testimony" as a new, post-verdict expert could have. Moreover, the evidence presented demonstrated a high probability of the defendant's guilt.**

WORDS AND PHRASES: INEFFECTIVE ASSISTANCE OF COUNSEL, EXPERT OPINION

***State v. Dingham,* 202 P.2d 388 (Wash. Ct. App. 2009). The defendant appealed from a conviction for theft and money laundering. The trial court had denied the defendant's requests for access to computer information in a format other than that used by the State. Noting the State's obligation to provide meaningful access to hard drive copies, the Court of**

Appeals reversed the conviction. The defense was entitled to use its own systems in analyzing the computer information.

WORDS AND PHRASES: DISCOVERY

***State v. Huggett,* 2010 WL 1287034 (Wisc. Ct. App. Apr. 6, 2010). The defendant had been charged with second-degree murder. At the time of the murder, a police officer seized the defendant's cell phone and took the cell phone of the defendant's girlfriend. The phones allegedly contained text and voice messages from the victim that would have supported self-defense and defense of another. Although the State preserved the text messages, it did not preserve any voicemail. In affirming the dismissal of the charge with prejudice, the appellate court held that the State had created an "expectation of preservation" by taking possession of the phones, that the State had failed in its duty to preserve, and that there was a due process violation as no "comparable evidence" existed. The tone of the victim was important, and neither text messages nor witness testimony was a replacement.**

WORDS AND PHRASES: DUTY TO PRESERVE

***State v. Lyons,* 2010 WL 4823676 (N.J. App. Div. Nov. 30, 2010). The trial court granted a motion to dismiss the Indictment, concluding that the defendant's "passive conduct" in possessing images of child pornography in a shared folder on a peer-to-peer network were insufficient to show intent to transfer or distribute the images to other. The Appellate Division reversed in a case of first impression in New Jersey and, in doing so, canvassed the law of other jurisdictions. The defendant was aware that his folder materials were available to others who shared the network and he acted "affirmatively" in installing the network and making these available to others.**

WORDS AND PHRASES: SCIENTER

***State v. McCraney,* 2010 WL 5140789 (Ohio Ct. App. Dec. 15, 2010) (*per curiam*). This is an appeal from the conviction of two defendant for criminal gang activity and other crimes. The Court of Appeals held, among other things, that evidence of photos posted on the defendants' MySpace pages (which showed them in gang-related conduct and attire) was sufficient to support the convictions.**

WORDS AND PHRASES: SUFFICIENCY OF EVIDENCE

State v. Reid, **945 A.2d 26 (N.J. 2008). Here, the State appealed from the suppression of evidence secured through a defective municipal court subpoena. The defendant had been indicted for computer theft after allegedly accessing a supplier's website and changing her employer's password and shipping address. In a case of first impression, the New Jersey Supreme Court held that Internet subscribers had a reasonable expectation of privacy in their IP addresses under the State Constitution. The court also held that disclosure of such addresses to third-party service providers did not vitiate the privacy interest and that the address be sought through an *ex parte* grand jury subpoena. Of interest, the court noted: "Should that reality [the existence of websites which reveal service providers but not individual users] change over time, the reasonableness of the expectation of privacy in Internet subscriber information might change as well."**

WORDS AND PHRASES: REASONABLE EXPECTATION OF PRIVACY

State v. Rivera, **2010 WL 339811 (Ohio. Ct. App. Feb. 1, 2010). The defendant appealed from his conviction for compelling prostitution. Law enforcement had secured the defendant's cell phone number from minors he had solicited to perform sexual acts and had also secured the defendant's text**

messages with the minors from his cell phone service provider. Thereafter, a search warrant was issued and the defendant confessed. On appeal, the conviction was affirmed. First, although the Stored Communications Act had been violated when law enforcement secured the messages by order rather that warrant and had not given the defendant notice, the Act did not provide a suppression remedy for violation of its terms. Moreover, the defendant did not demonstrate a privacy right in the messages.

WORDS AND PHRASES: STORED COMMUNICATIONS ACT, FOURTH AMENDMENT, REASONABLE EXPECTATION OF PRIVACY

***State v. Smith*, 2010 WL 5033513 (Mo. Ct. App. Dec. 28, 2010). Text messages between defendant and detective posing as a fourteen-year-old girl were admissible at trial for enticing a child and attempted statutory rape. Defendant objected to the admission of the texts on relevance grounds (so not relevant to ESI) and also for lack of foundation that the phone and records were in the same condition (because the detective deleted text messages to free up space for more texts). The court held that the detective properly authenticated the cell phone, which was admitted only to show the phone that was used as an instrumentality of the**

crime. The court rejected the foundational objections to the texts being deleted, holding that the texts themselves (admitted through properly authenticated photographs), not the content of the phone, were the relevant evidence.

WORDS AND PHRASES: ADMISSIBILITY

***State v. Smith,* 920 N.E.2d 949 (Ohio 2009). When the defendant was arrested a cell phone was found on his person. Thereafter, without obtaining a warrant, the State searched the information in the cell phone and found incriminating information. The defendant was convicted of drug possession and trafficking after the trial court denied his motion to suppress the information. In a case of first impression, the Ohio Supreme Court reversed the conviction. The court held that, under the Fourth Amendment, the cell phone was not the equivalent of a closed container that would justify a search incident to arrest, that the defendant had a legitimate expectation of privacy in the cell phone's contents, and that the State should have secured a warrant.**

WORDS AND PHRASES: REASONABLE EXPECTATION OF PRIVACY

END OF DOCUMENT