ADDITIONAL DEVELOPMENTS—PRIVACY LAW

COMPUTER FRAUD AND ABUSE ACT

In 1986, Congress enacted the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, as a way of combating computer crimes, particularly hacking. As computer crimes become more sophisticated, the broadly-written CFAA has been expanded by prosecutors and courts to address a range of new harms. Specifically, courts have varied in their interpretation of the "without authorization" provision in light of the lack of any statutory definition. Courts' struggles to consistently define the CFAA have resulted in several recent circuit splits over the meaning of "without authorization" in the employment context.

In *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), employer LVRC Holdings sued its former employee Brekka for emailing company documents from his work computer to himself and his wife while employed at the company. LVRC Holdings argued that Brekka's use of the computer for personal interests was without authorization. The court disagreed with a Seventh Circuit decision, *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), and held that Brekka had been given permission to use the computer and access those documents on grounds of his employment and therefore did not access a computer "without authorization," nor exceeded authorized access. Recently, the Fifth Circuit in *United States v. John*, 597 F.3d 263 (5th Cir. 2010), discussed *Brekka*, holding that a user can be held liable under the CFAA without ambiguity at least when "[a]n authorized computer user 'has reason to know' that he or she is not authorized to access data or information in furtherance of a criminally fraudulent scheme."

UNITED STATES V. COMPREHENSIVE DRUG TESTING, INC.

621 F.3d 1162 (9th Cir. 2010)

On September 13, 2010, the Ninth Circuit abrogated its prior en banc rehearing of United States v. Comprehensive Drug Testing, Inc. The case involved the government's seizure of computer records from a company that allegedly provided steroids to professional baseball players. The en banc decision relaxed the prior standard for issuing and executing search warrants and subpoenas for electronically stored information. This case interpreted the plain view doctrine and its application to electronic documents. The plain view doctrine allows an officer to seize—without a warrant—evidence and contraband found in plain view during a lawful observation.

In 2008, the Ninth Circuit heard a case involving the government's seizure of drug test records for hundreds of players in Major League Baseball (known as "the Tracey directory"). The question was whether these records—as well as related separately filed subpoenas—were admissible evidence in an ongoing grand jury investigation into the Bay Area Lab Cooperative's ("BALCO") alleged illegal doping of professional baseball players. The court held that the search of the Tracey directory did not violate the Fourth Amendment protection against unreasonable searches and seizures for three reasons: (1) "the government submitted detailed affidavits describing the anticipated difficulties of sorting computer data on-site" and "proposed a protocol to guide and to limit the seizures of intermingled evidence," (2) the government "complied with the protocol in the warrant," and (3) instead of seizing CDT's hardware (which was permissible by the warrant), the government only "copied several intermingled documents, including the Tracey directory." CDT appealed this decision and the court granted an en banc hearing.

The first en banc decision limited as admissible only evidence on the ten originally suspected players. Chief Judge Kozinski bound magistrate judges to strict procedural guidelines for digital searches that required the government to: (1) "forswear reliance on the plain view doctrine [that may allow it access to data beyond the scope of the warrant]"; (2) "fairly disclose the actual degree of . . . risks [of concealment and destruction of evidence]"; (3) design "the process of sorting, segregating, decoding and otherwise separating seizable data (as defined by the warrant) from all other data . . . to achieve that purpose and that purpose only." Furthermore, (4) "the warrant application should normally include . . . a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown." Finally, (5) "[o]nce the data has been segregated (and, if necessary, redacted), the government agents involved

in the investigation may examine only the information covered by the terms of the warrant." The court further held that "any remaining copies [of the data] must be destroyed" or "returned along with the actual physical medium that may have been seized (such as a hard drive or computer)."

A second en banc panel loosened these restrictions holding that they did not strictly bind magistrate judges. Granting magistrate judges more discretion in deciding what is or is not unreasonable under the plain view doctrine, the second panel held that judges must use the five procedural safeguards as guidelines, rather than requirements.

This decision represents the latest in a developing circuit split regarding what constitutes an unreasonable search and seizure under the Fourth Amendment. In early 2010, the Fourth Circuit held that digital evidence was to be treated the same as physical documents in *United States v. Williams*, 592 F.3d 511 (4th Cir. 2010). That is, incriminating files beyond the scope of the warrant that come into view are admissible. The Tenth Circuit in *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), held that the court should ask the conducting officer after the fact if they had actually been searching beyond the scope of the warrant. The Seventh Circuit's approach in *United States v. Mann* refrained from issuing a bright-line rule and limited their holding to the specific facts of that case. They, however, articulated that the file type specified in the warrant and the officer's subjectivity regarding whether they were looking for information authorized by the warrant at the time that they came across incriminating data did have bearing on the Fourth Amendment inquiry.

UNITED STATES V. WARSHAK

631 F.3d 266 (6th Cir. 2010)

The Sixth Circuit's decision in *Warshak* addressed whether the Fourth Amendment applies to email in guarding against unreasonable searches and seizures. The Court held that defendant Warhsak enjoyed a reasonable expectation of privacy in his email and government agents violated his Fourth Amendment rights through a warrantless, *ex parte* seizure of approximately 27,000 private emails from his internet search provider (ISP).

Warshak, the owner and founder of Berkeley Premium Nutraceuticals, faced criminal charges largely stemming from the deliberate manipulation of the company's charge-back ratio, a ratio determined by the percentage of transactions in a given 30-day period that result in a charge-back (customers asking their credit cards to cancel the transaction). This company's most famous drug was the 'male enhancing' product Enzyte. Due to a high level of customer dissatisfaction from the company's auto-ship program, the "life

blood" of the company business that placed unwitting customers into an opt-out monthly subscription service for Berkeley's herbal drugs, the company needed to stave off termination of its merchant-bank accounts that would result if too many customers charged-back their orders. Warshak and several others concocted a number of strategies to artificially inflate the number of sales transactions to reduce their charge-back ratio and obfuscate their high financial risk to banks; for instance they split a single transaction into many smaller transactions and also charged single dollar amounts to Warshak's own credit card.

Email constituted a vital piece of evidence for the government's criminal case. Through the use of the Stored Communications Act ("SCA"), which "permits a 'governmental entity' to compel a service provider to disclose the content of [electronic] communications in certain circumstances," the government compelled Warhsak's ISP to turn over his emails without notice to him. But, the court ruled such actions violated the Fourth Amendment as Warshak "plainly manifested an expectation that his emails would be shielded from outside scrutiny" and that such expectations are objectively reasonable. Thus, the Sixth Circuit held that "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional."

Nonetheless, because government agents relied in good faith on the provisions of the SCA, the exclusionary rule did not apply against Warshak's incriminating emails. The Court noted that the good faith reliance exception serves to avoid holding officers "accountable for mistakes of the legislature," unless a "reasonable officer should have known that the statute was unconstitutional." The Court ultimately affirmed Warshak's numerous criminal convictions resulting in a sentence of twenty five years.