



**Nick Akerman**

(212) 415-9217 ▪ akerman.nick@dorsey.com

Nick is a partner in the New York office of Dorsey & Whitney.

For additional articles like this one or to watch my one hour CLE seminar video go to:  
<http://computerfraud.us>



---

## **Sarah Palin Hacker’s Conviction Stands for Accessing Her Yahoo Email Account**

The college student David C. Kernell who was convicted by a Chattanooga, Tennessee jury of various federal crimes including a violation of the Computer Fraud and Abuse Act (“CFAA”) for accessing Alaska Governor Sarah Palin’s Yahoo email account will be sentenced on October 29, 2010. What Kernell did was to decipher the password for Alaska Governor Sarah Palin’s Yahoo email account and distribute her emails over the Internet during the 2008 Presidential campaign. Kernell moved post-verdict pursuant to Rule 29, Fed.R.Cr.P. for a judgment of acquittal on the ground that the evidence was insufficient to support his conviction. The trial court just last month denied Kernell’s motion finding that there was sufficient evidence to convict. *U.S. v. Kernell*, 2010 WL 3937421 \*4-5 (E.D. Tenn. Sept. 23, 2010). What is interesting about the court’s opinion is not what it says but what it does not say.

The motion directed at the CFAA was made on a very narrow ground challenging only whether Kernell had accessed a “protected computer.” This is an extremely weak defense since the Eight Circuit has recognized that “[e]very cell phone and cell tower is a “computer” under this statute’s definition; so is every iPod, every wireless base station in the corner coffee shop, and many another gadget.” *U.S. v. Mitra*, 405 F.3d 492, 495 (8<sup>th</sup> Cir. 2005)

The section of the CFAA upon which Kernell was convicted is 18 U.S.C. §1030(a)(2)(C) which makes it a crime for anyone who “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication.”

In pressing his motion to overturn the jury verdict Kernell claimed that the government had “failed to prove the ‘protected computer’ element . . . of [the crime]. . . because Yahoo! either would or could not identify the computer or computers on which the account and its attachments resided.” *U.S. v. Kernell* at \*5. In rejecting Kernell’s motion the court relied on the trial evidence of the “Yahoo! records [that] revealed that the computers managing the Account on the date of the offense were located in Quincy, Washington.” *Id.* The court emphasized that Kernell “does not dispute that a Yahoo! computer located in Quincy, Washington was managing the Account at that time.” *Id.* In addition, “[t]he records also showed that Defendant accessed the Account by using Internet Protocol address “66.253.190 .21.” *Id.*

The court concluded “[i]t was not necessary for the Government to identify the specific Yahoo! computer that managed the Account because: (1) the location of the Yahoo! computer was verified; and (2) the IP address used by the Defendant to access the Account was verified.” Based on that evidence, the court held “that a rational trier of fact, when viewing the evidence in

the light most favorable to the Government, could have found the essential elements of the” CFAA count. *Id.*

What is absent from this opinion is any defense that Kernell could have raised before the jury based on unauthorized access, a critical element of the CFAA. According to the press reports, Kernell was able to determine Palin’s Yahoo email address from publicly available information disseminated by Governor Palin about her background. Given her creation of a password based on facts provided to the entire world, a factual defense could have been raised that she gave everyone constructive access to her account. There is no mention in the opinion of any such defense having been advanced.