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

Nick is a partner in the New York office of Dorsey & Whitney. This article was co-authored with Melissa Krasnow, a partner in the Minneapolis office of Dorsey & Whitney

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

DORSEY
DORSEY & WHITNEY LLP

Will News Corp. Executives and Reporters Be Charged with Criminal Violations of the Computer Fraud and Abuse Act?

The *New York Times* recently reported that the UK telephone hacking scandal could result in News Corp. and its executives being charged in the United States with criminal violations of the Foreign Corrupt Practices Act, Title 15, U.S.C. § 78m, the Electronic Communications Privacy Act, 18 U.S.C. § 2511, and the Telephone Records and Privacy Protection Act, 18 U.S.C. § 1039. See *NYT*, "News Corp. Braces for Legal Trouble in the U.S.," July 18, 2011. What the *New York Times*, as well as all of the politicians and pundits who have commented on this issue, failed to mention is that the federal Computer Fraud and Abuse Act ("CFAA") is the federal criminal statute that most neatly fits the alleged crimes of hacking into voice mails and telephone records. Title 18, U.S.C. §1030.

The CFAA is the omnibus federal computer crime statute that, among other things, 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." §1030(a)(2)(C). There is little doubt that the information News Corp.'s reporters allegedly obtained, the voices mails and telephone records, were data files from computers, and there is also no question that the access to the computers through which the News Corp. reporters allegedly obtained the voice mails and telephone information was not authorized.

The CFAA's definition of a "computer" covers every conceivable type of computer. §1030(e)(1). As the defendant correctly claimed in *U.S. v. Mitra*, 405 F.3d 492, 495 (8th Cir. 2005), "[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." Thus, it is highly likely that from whatever type of computer the News Corp.'s reporters retrieved the voices mails and other personal information, it almost certainly came from what the CFAA would recognize as a computer.

As stated above, to be guilty of the crime the reporter must not only have accessed a computer, but that the information be obtained from a "protected computer," defined by the CFAA as a computer "used in interstate or foreign commerce or communication." §1030(a)(2)(B). But what is of particular relevance to the News Corp. situation is that this definition extends to any computer "located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." In other words, any computer

anywhere in the world that communicates with the United States through email is subject to the CFAA and can form the basis for a criminal prosecution in the United States.

While it is theoretically possible that a News Corp. reporter could be charged with criminal violations of the CFAA for accessing a computer in the UK, it is highly unlikely that the Department of Justice would prosecute a case that thus far appears to be solely a UK crime. However, to the extent the current FBI investigation uncovers evidence of any U.S. connection such as the alleged retrieval of voices mails from 9/11 victims, the CFAA is likely to be the Justice Department's criminal statute of choice for the News Corp. reporters and executives who initiated the hacking.

`