



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>



Unauthorized Access of President Obama’s Student Loan Data Ends in Computer Fraud Conviction

The Eight Circuit Court of Appeals upheld the criminal conviction of Sandra Teague for accessing President Obama’s data in the National Student Loan Data System during her employment at a government contractor for the Department of Education. *U.S. v. Teague*, 646 F.3d 1119 (8th Cir. 2011). She was indicted and convicted by a jury for one count of exceeding unauthorized access to a computer in violation of 18 U.S.C. § 1030 (a)(2)(B), of the Computer Fraud and Abuse Act (“CFAA”). This section of the CFAA makes it a crime to intentionally exceed authorized access to a computer and obtain information from a department or agency of the government. She was sentenced to two years probation. This decision is significant not because the victim of the computer intrusion was the President of the United States, but because it greatly expands the breadth and reach of the CFAA.

The proof at trial was wholly circumstantial, but, as the court found, was sufficient for the jury to convict. As the court explained, “the government introduced evidence establishing that on August 27, 2008, Teague's user ID accessed Obama's records, as well as the records of Marc Martin, Teague's nephew. Critically, Teague admitted to conducting the Marc Martin search. Furthermore, the government introduced testimony that there was no timeout between the Obama search and the Marc Martin search. Based on this cumulative evidence, the jury could reasonably conclude the Obama search, which was part of one continuous session with the Marc Martin search, was also conducted by Teague.” *Id.* at 1122. In affirming the conviction the court also relied on Teague’s trial testimony that “was not particularly credible” and her false exculpatory statements to Department of Education Agents. *Id.*

What is significant about the proof in this case is the lack of any evidence that Teague did anything with the information she accessed. The proof at trial only showed that she had viewed Obama’s student loan records, not that she published it, used it or did anything with it. Based solely on her viewing the Obama student loan data, the court found the government had proved the critical CFAA element of having obtained information. Obtaining information is not only a critical element to prove unauthorized access to a government computer but is also a critical element to prove both certain criminal and civil violations of the CFAA for unauthorized access to private computers.

While not acknowledged by *Teague*, this decision is at odds with the First Circuit’s ruling 14

years ago in *U.S. v. Czubinski*, 106 F.3d 1069, 1078 (1st Cir. 1997) in which the court held that there was insufficient proof to affirm a CFAA conviction when Czubinski, an IRS employee, had exceeded his authorized access to the IRS computer but “merely” viewed restricted tax information relating to “friends, acquaintances, and political rivals.” There must be a “showing of some additional end-to which the unauthorized access is a means.” *Id.*

Ultimately, the U.S. Supreme Court may have to resolve this split in the two circuit opinions. Based on recent precedent, most notably *Morrison v. National Australia Bank, Ltd*, 130 S.Ct. 2869 (2010), the Supreme Court, having warned against judicial legislating by engrafting requirements on a statute that are not supported by the plain language of the statute, is likely to side with *Teague*. There is nothing in the plain language of the CFAA that requires proof of “some additional end to which the unauthorized access is a means.” It simply requires proof of obtaining information.

Also, in light of privacy concerns and the dangers posed by the use of memorized data taken from the unauthorized access to computers, there is no good policy reason not to interpret “obtaining information” as simply viewing it. By adopting the 1st Circuit’s limitation on the CFAA, there is nothing to stop the low-tech computer thief -- someone who uses a cellphone to record the viewed data or copies it down with pen and paper with no evidentiary traces left on the computer. In short, this case correctly broadens the reach of the CFAA beyond the 1st Circuit’s view in 1997 and is the likely view to be adopted by the Supreme Court.