THE BUZZ
REDGRAVE LLP
ON INFORMATION MATTERS

APRIL 17, 2012

A Look at 3 Cases: U.S. v. Drew, U.S. v. Nosal and U.S. v. Aleynikov

U.S. v. Drew

In the fall of 2006, Lori Drew created a false identity within a MySpace account and used it to cyberbully Megan Meier, Drew's daughter's former friend. Megan Meier committed suicide,[1] the public was outraged,[2] and Drew was federally prosecuted under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, for her alleged use of a computer in excess of authorized use.[3]

The circumstances involved in the *Drew* case were both gripping and tragic, and struck a chord with tens of millions of parents around the country and the world.[4] However, as acknowledged by many commentators, "bad cases [can] make bad law,"[5] and when the dust settled, the Justice Department was left trying to find a federal law with which to prosecute Drew.[6] While Drew was convicted under the CFAA, a California federal judge later acquitted her, finding that her convictions would effectively "criminalize…a breach of contract."[7]

Charges under the CFAA and like federal statutes were explicitly at issue in two recent opinions: in the Ninth Circuit *U.S. v. Nosal*[8] matter and the Second Circuit *U.S. v. Aleynikov*[9] matter. While the alleged actions of the defendants in both matters seem facially "wrong" and worthy of some sort of punishment, these opinions should remind attorneys that federal crimes are "creatures of statute."[10] That is, even if behavior seems reprehensible and even if the public believes that "something should be done," a federal case requires a federal statute with an applicable federal crime. If none exists, improper federal counts are properly challenged and judges will dismiss them.

---

[1] T. Jones, *A Deadly Web of Deceit*, The Washington Post, January 10, 2008 (http://www.washingtonpost.com/wp-dyn/content/article/2008/01/09/AR2008010903367_pf.html).
[2] K. Zetter, *Cyberbullying Suicide Stokes the Internet Fury Machine*, WIRED – Politics, November 21, 2007 (http://www.wired.com/politics/onlinerights/news/2007/11/vigilante_justice).
[3] *See U.S. v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009)
[4] I. Munro, *How Lori Drew became America's most reviled mother*, The Age – TECH, December 1, 2007 (http://www.theage.com.au/news/web/americas-most-reviled-mother/2007/11/30/1196394672124.html).
[5] J. Morris, *A girl's suicide is a very tragic case, but should it be a "federal case"?*, Center for Democracy & Technology, May 16, 2008. (https://www.cdt.org/blogs/john-morris/girls-suicide-very-tragic-case-should-it-be-federal-case). See also, F. Schauer, *Do Cases Make Bad Law?* KSG Working Paper No. RWP05-013, February 2005 (http://ssrn.com/abstract=779386 or http://dx.doi.org/10.2139/ssrn.779386).
[6] L. Harris, *You May Already Be a Criminal*, ABC News – Tech This Out, May 22, 2008. (http://abcnews.go.com/Technology/story?id=4903596&page=1).
[7] K. Zetter, *Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury*, WIRED Threat Level, July 2, 2009 (http://www.wired.com/threatlevel/2009/07/drew_court/).
[8] *U.S. v. Nosal*, No. 10-10038 D.C. No. 3:08-cr-00237-MHP-1 (9th Cir. April 10, 2012).
[9] *U.S. v. Aleynikov*, No. 11-1126 (2nd Cir. April 11, 2012).
[10] *Dowling v. U.S.*, 473 U.S. 207, 213 (1985).

U.S. v. Nosal

David Nosal had worked at the executive search firm of Korn/Ferry, but left to start a competing business. After his departure, Nosal convinced former colleagues—still at Korn/Ferry—to use their log-in credentials to "download source lists, names and contact information from a confidential database on the company's computer" and transfer that information to Nosal. Importantly (for the case) the former colleagues were authorized to access the database; however, Korn/Ferry did have a policy that forbade disclosing confidential information.

Nosal was indicted on twenty counts, including violations of the CFAA—specifically 18 U.S.C.§ 1030(a)(4)—for aiding and abetting his former Korn/Ferry colleagues in "exceed[ing their] authorized access" with intent to defraud. The Ninth Circuit's *en banc* opinion addressed the CFAA counts and evaluated whether Nosal's colleagues' otherwise-authorized access to the database changed in character because of the colleagues' subsequently successful intent to share the information with a competitor. That is, Nosal's colleagues could access the database legitimately without a violation of the CFAA; however, once they accessed that very same database while determined to share its information (as demonstrated by their actual sharing), did that identical behavior become criminal under the CFAA?

In a narrow reading of the statute, Chief Judge Alex Kozinski wrote that the plain language of the CFAA targets the "unauthorized *procurement* or alteration of information, not its misuse or misappropriation."[11] (emphasis added). Therefore, held the court, the CFAA's phrase "'exceeds authorized access' does not extend to violations of use restrictions"—and "the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*."[12] (emphasis in original).

Nosal's colleagues' otherwise-authorized access to the database did not become criminal activity when their intent changed. In so holding, the Ninth Circuit was acutely aware of the "bad facts make bad law" maxim that infused the *Drew* matter. And when addressing the opposing view, held by the Eleventh, Fifth, and Seventh Circuits, the court found that those "courts looked only at the culpable behavior of the defendants before them," failing to consider the effects of those decisions on "millions of ordinary citizens."[13]

U.S. v. Aleynikov

Sergey Aleynikov was a computer programmer for Goldman Sachs & Co. Aleynikov developed the source code for Goldman's proprietary high-frequency trading ("HFT") system, specifically the infrastructure programs facilitating the flow of information throughout the trading system and

[11] *U.S. v. Nosal*, No. 10-10038 D.C. No. 3:08-cr-00237-MHP-1, at 3871, *15 (9th Cir. April 10, 2012).
[12] *Id.* at 3872, *16.
[13] *Id.* at 3871, *15.

monitoring the system's performance. Aleynikov left Goldman for a more lucrative opportunity, and on his last day of work at Goldman:

> Aleynikov encrypted and uploaded to a server in Germany more than 500,000 lines of source code for Goldman's HFT system, including code for a substantial part of the infrastructure, and some of the algorithms and market data connectivity programs. Some of the code pertained to programs that could operate independently of the rest of the Goldman system and could be integrated into a competitor's system. After uploading the source code, Aleynikov deleted the encryption program as well as the history of his computer commands.[14]

His actions were discovered quickly, and Aleynikov was charged with violating the Economic Espionage Act of 1996 (the "EEA"), 18 U.S.C. § 1832(a), the CFAA 18 U.S.C. § 1030, and the National Stolen Property Act (the "NSPA"), 18 U.S.C. § 2314.

As in *Nosal*, Aleynikov had proper access to the information he downloaded at the time he downloaded it. But in contrast with the district court in *Nosal*, the CFAA count was dismissed when the *Aleynikov* district court found that Aleynikov's access to the Goldman computer did not exceed the scope of his authorization, and that authorized use of a computer, even when it misappropriates information, is not an offense under the CFAA.[15]

The Second Circuit also found that Aleynikov did not violate either the NSPA or the EEA. When evaluating the NSPA, the court held that because Aleynikov's theft of computer code did not involve assuming "'physical control' over" the code, and did not "'deprive [Goldman] of its use,' Aleynikov did not violate the NSPA."[16] Then, further acknowledging that Aleynikov "should have known [that he] was in breach of his confidentiality obligations to Goldman, and was dishonest in ways that would subject him to sanctions," the court still found that Aleynikov "could not have known that [his behavior] would offend [the EEA]."[17]

Have the decisions in *Nosal*, *Aleynikov*, and *Drew* influenced changes in the CFAA or like statutes? Not so far. While President Obama pushed for further changes to CFAA as recently as May of 2011, Senators P. Leahy (D-Vt.) and A. Franken (D-Minn.) asked for modifications to definitions and acknowledged the concerns about the potential criminalization of terms-of-service agreements.[18] There have been no further updates on any CFAA change progress. Perhaps the failed application of CFAA and similar federal statutes in the commercial context will be a properly financed spur to include greater specificity in the next

---

[14] *U.S. v. Aleynikov*, No. 11-1126, at *5 (2nd Cir. April 11, 2012).
[15] *U.S. v. Aleynikov*, 737 F. Supp. 2d 173, 192-194 (S.D.N.Y. 2010).
[16] *U.S. v. Aleynikov*, No. 11-1126, at *18 (2nd Cir. April 11, 2012).
[17] *Id.*, at *28.
[18] G. Gross, *Senators push for changes in cybercrime law*, TechWorld (IDG News Service), September 8, 2011 (http://www.techworld.com.au/article/400054/senators_push_changes_cybercrime_law/).

iterations of these statutes. Or perhaps it will take another public outcry in the vein of *Drew* to incentivize congress to criminalize online behavior.

Contact Us: For further information or if you have any questions regarding this Alert, please contact your Redgrave LLP attorney or Managing Partner Victoria Redgrave at (202) 681-2599 or vredgrave@redgravellp.com.