Fear and Trade Secrets on the Campaign Trail

Insights
4.26.18

The Democratic National Committee recently filed a lawsuit against Russia, WikiLeaks, the Trump Campaign, and a bunch of individuals (including Julian Assange, Jared Kushner, and a hacker named "Guccifer 2.0") that includes claims of trade secret violations. The April 20 lawsuit alleges an alphabet soup of claims—CFAA, SCA, DMCA, RICO, among others—mostly based on the premise that Russian operatives successfully hacked the DNC's computers, stole politically sensitive information, and then destabilized the American political system in conjunction with the Trump campaign and WikiLeaks.

The two trade secret claims in the lawsuit include a claim that Russia, Guccifer 2.0, WikiLeaks and Assange violated the Defend Trade Secrets Act (DTSA), 18 U.S.C. § 1836 et seq., and that all defendants—including the Trump Campaign, Jared Kushner, and Donald Trump, Jr.—violated the Washington D.C. Uniform Trade Secrets Act, D.C. Code Ann §§ 36-401 – 46-410.

In his classic account of the 1972 presidential campaign, Hunter S. Thompson cautioned that "every now and then you have to get away from that ugly Old Politics trip, or it will drive you to kicking the walls and hurling AR3's into the fireplace." I'll take HST's advice here and stay away from the Old Politics of the DNC lawsuit. Instead, I'll focus on the potential hurdles the DNC faces in succeeding on its trade secrets claims. That should keep us far enough away from exploding fireplaces.

Were the DNC's stolen documents "trade secrets"?
Under the DTSA, a "trade secret" is any type of "financial, business, scientific, technical, economic, or engineering information" that "derives independent economic value . . . from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information."

The DNC's lawsuit alleges that its trade secrets included "confidential proprietary documents related to campaigns, fundraising, and campaign strategy." The lawsuit mostly glosses over exactly which documents and information it claims were trade secrets. Specific documents that the DNC lawsuit does reference include: (1) a DNC-authored opposition research report on Donald Trump from December 2015; (2) DNC strategy documents related to the DNC's "counter-convention" to the RNC convention; (3) personal information—including social security and passport numbers—of individuals who communicated with or donated to the DNC; and (4) Clinton campaign chairman John Podesta's hacked emails.

The key questions will be whether these documents, or any others that the DNC identifies throughout the litigation, had any independent economic value, and whether the information in the documents was not generally known or readily ascertainable through proper means. The courts have not had much opportunity to analyze the meaning of trade secrets in the political context, but it seems likely that information such as donor and email lists could be protected trade secrets.

For instance, a political fundraising consultant was held liable for trade secret misappropriation in a recent case from Alaska. In that case, an arbitrator held that an advocacy organization's donor lists and email listings were protectable trade secrets. *Kaplan v. Renewable Resources Coalition, Inc. (In re Kaplan)* (Dec. 9, 2016, B.A.P. 9th Cir.).

Congressman Mike Honda (D-CA) took a similar approach in a 2016 lawsuit alleging that a former intern took and used his donor list to attack him and recruit support for his opponent. However, the parties settled that case before a court could decide whether the donor list at issue was a protectable trade secret.

In the same vein, voter contact firm Winning Connections sued former employees who left to start a competing firm. In the lawsuit, Winning Connections alleged that the former employees misappropriated trade secrets, including customer lists, marketing information, existing contracts and prices, and revenue and growth information. As with Congressman Honda's lawsuit, the Winning Connections suit settled before the court could weigh in on whether the alleged trade secrets were in fact protectable.

Did the DNC take reasonable measures to keep its information secret?

If the DNC successfully demonstrates that the stolen information includes trade secrets, it will then need to prove that it took reasonable measures to keep its information secret and protected. In lower-profile cases, courts have found that password-protecting computers and servers, contractually binding staffers to confidentiality agreements, and limiting remote access to network servers could satisfy this requirement. However, disclosure of alleged secrets—for instance, forwarding emails to outside parties or disclosing alleged secrets to outside parties—could torpedo a trade secret claim.

The DNC alleges that it took reasonable measures to keep its stolen information secret. The lawsuit alleges that the DNC maintained its information on secure, password-protected servers, trained staff on best practices for keeping the information secure, and required staff to sign confidentiality agreements. Importantly, the "reasonable" standard is flexible and depends on the circumstances of each case. The DNC's measures may have been reasonable in lower-profile circumstances. But it is unclear whether a court would hold the DNC to a higher standard for protecting its confidential information—particularly given that it was a presidential campaign, not a run-of-the-mill business—and that it was apparently warned of cyberattack threats during the 2016 campaign.

Conclusion

Damages under the DTSA and D.C. Trade Secrets Act can include actual losses, punitive damages, attorneys' fees, and injunctive relief. Given the domestic and geopolitical stakes, there is no doubt this will be a fact-intensive and highly contested lawsuit. Add to that cocktail some stiff pours of Trump-era politics and international espionage, and we've got a situation to keep our eyes on.

Related People

Corey J. Goerdt
Director of Pro Bono & Community Engagement
404.240.4212
Email