The U.S. Court of Appeals for the Ninth Circuit Upholds Qatar's Sovereign Immunity in Cyberespionage Case

The Ninth Circuit's recent decision in *Broidy Capital Management v. Qatar* affirmed dismissal of claims that Qatar hacked the plaintiffs' computers and disseminated stolen information on grounds that Qatar was entitled to sovereign immunity under the U.S. Foreign Sovereign Immunities Act ("FSIA").[1]

The Alleged Acts of Cyberespionage

The plaintiffs, Broidy Capital Management and its CEO Elliott Broidy, claimed that they were targeted in a Qatari cyberespionage scheme in retaliation for their outspoken criticism of Qatar and their attempts to influence the U.S. government's foreign policy towards Qatar.

According to the complaint, Qatar supposedly orchestrated a continuing series of cyberattacks on the plaintiffs' servers in California in order to steal confidential information. Qatar allegedly hired a New York firm, Global Risk Advisors ("GRA"), to help identify foreign hackers to coordinate the attacks. A forensic investigation discovered that most of the attacks originated in Qatar while others originated in Vermont. The plaintiffs alleged that Qatar disseminated information obtained in the cyberattacks to various media outlets who published a series of unflattering articles about the plaintiffs. The complaint asserted that a New York based public relations firm, Stonington Strategies ("Stonington"), participated in the dissemination of the stolen information.

The plaintiffs sued Qatar, GRA and Stonington in federal court in California, asserting claims under the U.S. Computer Fraud and Abuse Act and the California Comprehensive Computer Data Access and Fraud Act as well as common law tort claims for intrusion upon seclusion. The district court granted Qatar's motion to dismiss for lack of jurisdiction under the FSIA, finding that neither the FSIA's tort exception nor the commercial activity exception to immunity applied. The Ninth Circuit affirmed.

The Alleged Acts of Cyberespionage Fell Within the "Discretionary Function" Exemption of the FSIA's Tort Exception to Immunity

The FSIA's tort exception abrogates immunity with respect to torts claims against foreign states seeking monetary damages for personal injury or property damage caused by a tortious act or omission occurring in the United States.[2] The district court in

---

[1] *Broidy Capital Management v. Qatar*, 982 F.3d 582 (9th Cir. 2020).

[2] 28 U.S.C. § 1605(a)(5).

Broidy declined to apply the tort exception because it found that the alleged hacking was orchestrated from abroad and therefore did not occur in the United States. While the Ninth Circuit affirmed this finding, it did so on different grounds. It held that Qatar's alleged conduct fell within the scope of the FSIA's so-called "discretionary function" exemption, which explicitly states that the tort exception does not apply to "any claim based upon the exercise or performance or the failure to exercise or perform a discretionary function regardless of whether the discretion be abused."[3]

The Ninth Circuit rejected the plaintiffs' argument that the discretionary function exemption is inapplicable where the foreign state's discretionary acts are alleged to have violated federal and state statutes. While the Ninth Circuit recognized that the discretionary function exemption does not apply where the alleged acts were "specifically proscribed by applicable law," it held that the state's domestic law and, possibly, established principles of international law are the relevant applicable law – and not U.S. law.

The Ninth Circuit held that the plaintiffs failed to allege that Qatar's alleged conduct violated Qatari law or international law. It found that the prohibitions against computer hacking under Qatari law did not bind government agents acting in accordance with official orders, explaining; "[I]t would perhaps be surprising if the domestic law of any country prohibited its own government agents from engaging in covert cyberespionage and public relations activities aimed at foreign nationals in other countries." The Ninth Circuit further held: "The status of peacetime espionage under international law is a subject of vigorous debate and the parties have not pointed us to any sufficiently clear rule of international law that would impose a mandatory and judicially enforceable duty on Qatar not to do what it allegedly did here." Thus, consistent with the Supreme Court's admonition in *Sosa v. Alavarez-Machain*[4] against recognizing new violations of international law, the Ninth Circuit declined to find Qatar's alleged conduct to violate international law.

Finally, while the Ninth Circuit recognized that the discretionary function exemption applies only where the challenged governmental actions were grounded in social, economic or political policy, it held that there was "little doubt that Qatar's alleged actions involved considerations of public policy" because Qatar allegedly "undertook the challenged actions as one component of a public-relations strategy to influence public opinion in the United States by curtailing the influence of individuals, such as Broidy, who could undermine the standing of the State of Qatar in the United States."

[3] 28 U.S.C. § 1605(a)(5)(A).

[4] *See Broidy* (citing *Sosa v. Alavarez-Machain*, 342 U.S. 692 (2004)).

Qatar's Cyberespionage and Public Relations Efforts Were Not "Commercial" in Nature

The Ninth Circuit also held that the FSIA's commercial activity exception did not apply. That exception abrogates immunity in actions against foreign states that are "based upon" a foreign state's commercial activities that either occurred in the United States or had a "direct effect in the United States."[5]

As "the 'crucial' first step" of the analysis under the commercial activity exception, the Ninth Circuit found that the complaint was "based upon" either the hacking of the plaintiffs' computers and/or the dissemination of stolen information. It explained that the fact that Qatar entered into contracts with U.S. firms in connection with these activities did not alone entitle the plaintiffs to any recovery and therefore Qatar's dealings with those U.S. firms were not the basis of the lawsuit.

The Ninth Circuit then held that neither the hacking of the plaintiffs' computers nor the dissemination of the stolen information constituted "commercial activity" for purposes of the FSIA. The statute defines "commercial activity" by reference to the nature of the activity and not its purpose,[6] and the U.S. Supreme Court held in *Weltover v. Republic of Argentina* that a foreign state's actions are commercial in nature where "they are the type of actions by which a private party engages in trade and traffic in commerce."[7] Nevertheless, the Ninth Circuit rejected the argument that computer hacking was "commercial" simply because private actors can engage in such conduct. Instead, the *Broidy* court looked to the "context" of Qatar's alleged actions and held that there is a distinction between engaging in conduct to harm a commercial rival and conduct designed to harm a policy critic of the state. It explained: "We have little difficulty in concluding that, without more, a foreign government's conduct of clandestine surveillance and espionage against a national of another nation in the other nation is not one in which commercial actors typically engage." It further held that Qatar's subsequent dissemination of the stolen information was not commercial in nature because it was tied to Qatar's policy objectives and there was no allegation that Qatar made commercial use of that information.

Impact of the *Broidy* Decision

The *Broidy* decision is notable in two respects. First, while other courts – including the district court in *Broidy* – have declined to apply the FSIA's tort exception in computer

[5] 28 U.S.C. § 1605(a)(2).

[6] 28 U.S.C. § 1603(d).

[7] *Weltover v. Republic of Argentina*, 504 U.S. 607 (1992).

hacking cases where the alleged hacking did not "occur[] in the United States" as required by the statute, the Ninth Circuit's application of the tort exception's discretionary function exemption would appear to provide a broader scope of immunity in cyberespionage cases.[8]

Second, the Ninth Circuit's "context" based approach to determining the commercial nature of a foreign state's conduct at first blush appears to be in tension with the Supreme Court's admonition in *Weltover* that a foreign state's purpose or motive is irrelevant to such an analysis. But *Weltover* dealt with conduct that was clearly commercial – the issuance of bonds. By contrast, the computer hacking alleged in *Broidy* was not inherently commercial in nature, and the Ninth Circuit's decision to look to the "context" of the activity is a common sense approach that requires courts to consider whether the foreign state acted as a commercial player when it engaged in conduct that is neither inherently commercial nor inherently sovereign in nature.

About Curtis

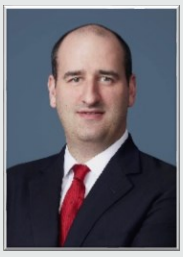
Curtis, Mallet-Prevost, Colt & Mosle LLP is a leading international law firm. Headquartered in New York, Curtis has 17 offices in the United States, Latin America, Europe, the Middle East and Asia. Curtis represents a wide range of clients, including multinational corporations and financial institutions, governments and state-owned companies, money managers, sovereign wealth funds, family-owned businesses, individuals and entrepreneurs.

For more information about Curtis, please visit www.curtis.com.

[8] *See Doe v. Fed. Democratic Republic of Ethiopia,* 851 F.3d 7, 11 (D.C. Cir. 2017); *Democratic Nat'l Comm. v. Russian Fed'n*, 392 F. Supp. 3d 410, 428 (S.D.N.Y. 2019); *see also Broidy Capital Mgmt., LLC v. State of Qatar,* No. CV 18-2421-JFW(Ex), 2018 U.S. Dist. LEXIS 226540, at *17 n.3 (C.D. Cal. Aug. 8, 2018) (tort exception did not apply because most of the cyber attacks allegedly originated in Qatar and the few attacks alleged to have originated in Vermont were merely a continuation of the attacks from Qatar).

Please feel free to contact any of the persons listed below if you have any questions on this important development:

Joseph D. Pizzurro
Partner
jpizzurro@curtis.com
New York: +1 212 696 6196



Kevin A. Meehan
Partner
kmeehan@curtis.com
New York: +1 212 696 6197

Juan O. Perla
Associate
jperla@curtis.com
New York: +1 212 696 6084