JULY 6, 2017

Unintended Plaintiffs: United States District Court Allows Private Citizens to Sue a Government Contractor For Failing to Adequately Safeguard Personal Information

, *Jon Neiditz*, and *Christian Henel*

In a remarkable opinion with potentially wide-ranging implications, the United States District Court for the District of Columbia recently allowed a member of the public to sue a federal government contractor directly for privacy violations the plaintiff allegedly suffered during the contractor's performance.

The Plaintiffs in *McDowell v. CGI Federal Inc.,* CA No. 15-1157 (Slip Op. June 1, 2017) were passport applicants who gave her personal information to State Department contractor CGI Federal, Inc. ("CGI"). CGI is a federal contractor that processes passport applications for the State Department. While CGI had a contract to provide passport application processing for the State Department, it never entered into any express or implied contract with the Plaintiffs. According to the Complaint, CGI failed to adequately safeguard her data when several CGI employees stole Plaintiffs' personal information and used it to counterfeit identify documents, obtain commercial lines of credit, and make fraudulent purchases. Plaintiffs sued CGI for (1) violations of the District of Columbia's Consumer Protection Procedures Act ("CPPA"); (2) negligence; (3) breach of contract; (4) breach of bailment; and (5) unjust enrichment. CGI moved to dismiss the claims on several grounds.

The Court dismissed four out of the five counts but kept the case alive by sparing the breach of contract count. The Court first dismissed the CPPA count, finding Plaintiffs ineligible to bring the CPPA count because they were not "consumers" as defined by that statute. It dismissed the negligence count because Plaintiffs failed to allege a "special relationship" with CGI sufficient to avoid D.C.'s "economic loss" bar to negligence claims. It dismissed the unjust enrichment count because Plaintiffs conferred no benefit upon CGI, and it dismissed the bailment count because Plaintiffs had no express or implied agreement with CGI to protect their data.

Despite finding no contract between Plaintiffs and CGI, the Court allowed the breach of contract suit to go forward. The Court reasoned that Plaintiffs were third-party beneficiaries of the contract between CGI and the State Department. Under D.C. law, a plaintiff can sue a contractor as a third party beneficiary if the contracting parties "clearly intended that the contract would benefit the plaintiff or an identifiable class to which the plaintiff belongs." (Slip Op. at 13). In *McDowell*, the District Court reasoned that CGI and the State Department clearly intended to protect Plaintiffs' data when CGI agreed in its

government contract to act reasonably and employ reasonable safeguards at all times to handle Plaintiffs' personal information. The Court noted that neither party attached a complete version of the CGI-State Department contract and warned that further scrutiny could result in a finding that CGI did not breach any obligation toward Plaintiffs. The Plaintiffs' allegations were sufficient, however, to survive CGI's motion to dismiss under the liberal pleading standard applied by Federal Courts. Thus, CGI won four-fifths of its motion to dismiss, but the practical result is that CGI continues to defend the lawsuit in federal court.

McDowell should serve as a cautionary tale of how government contractors handling private citizens' data and personal information could face direct liability to those citizens in the event of a data breach or privacy violation. The contractor in *McDowell* had no contract with the Plaintiffs, owed no duty in tort, and had no other bailment relationship or other special relationship with the Plaintiffs, but nonetheless found itself defending a lawsuit for failing to adequately safeguard their data. Our review of similar cases around the country indicates that private citizens are often willing to pursue contractors for data breach and privacy violations even in cases where the connection between the contractors and the citizens seems attenuated.

McDowell's ruling adds to what appears to be ever-increasing risk to government contractors handling private and personal information. In 2016, the U.S. Supreme Court indicated in *Spokeo v. Robins*, 136 S.Ct. 1540 (2016) that a private citizen may have standing to sue a third party for statutory violations (in that case, the Fair Credit Reporting Act) even if it has not suffered actual harm, as long as the *risk* of real harm is the type of risk Congress intended to curb when it passed the statute. Federal courts applying *Spokeo* have been divided over what kind and degree of damage a plaintiff must allege to demonstrate standing to sue. Some courts have attempted to narrow this exposure by dismissing cases where the Plaintiffs fail to allege a "concrete injury" resulting from the breach, while other courts have opened their doors to suits alleging intangible and even theoretical damages. Although *McDowell* did not directly address these standing issues (the Court dismissed the plaintiffs' CPPA count because they were not "consumers" under the statute), contractors should keep in mind that even the risk of harm could expose them to direct liability for data breaches and privacy violations.

Likewise, and regardless of their liability to private citizens, federal contractors remain liable to the Government directly for data breaches and privacy violations, where exposure may range from simple breach of contract damages and liquidated damages to more serious False Claims Act violations under the Supreme Court's evolving interpretation of false claims liability. *See Universal Health Services, Inc. ex rel. Escobar*, 136 S.Ct. 1989 (2016).

Although the lessons contractors should take from *McDowell* are simple, the consequences of underestimating the risk of liability to private citizens can be dire. Contractors handling individuals' personal information should consider the following points:

- Consider whether their contracts with federal agencies clearly assign responsibility for

safeguarding individuals' data and information. If it's unclear, assume that the contractor could be liable to individuals as third-party beneficiaries.

- Consider the feasibility of disclaiming or limiting liability for data breaches and privacy act violations at the time they receive the information or data from individuals. While this approach may not completely insulate the contractor, it would, at a minimum, reinforce the fact that accepting the data does not create any special relationship in tort or bailment.
- Ensure they are taking measures necessary to adequately safeguard the entrusted data. Refer to the safeguarding requirements in the applicable contract(s) and implement any other risk-based approaches reasonably necessary to limit exposure for data breaches or privacy violations. Consider what security controls the contractor actually has in place to safeguard the individual's data and test to ensure that those controls are turned on and effective.