JULY 24, 2018

Data breach class actions: Georgia appellate court again rejects negligence claim predicated on alleged duty to safeguard personal information

by Jay Bogan

Takeaway: Data breaches are now a fact of life, whether for card-carrying consumers or commercial entities victimized by hacking or otherwise required to deal with the consequences. Class action litigation often ensues, where tort claims such as claims for negligence and negligence per se are commonly asserted. Claims for negligence, however, require the breach of a recognized duty, and whether such a legal duty exists can turn on the statutes and case-law peculiar to a particular state. The Georgia Court of Appeals recently answered this question, ruling in *McConnell v. Georgia Department of Labor*, 814 S.E.2d 790, No. A16A0655, 2018 WL 2173252 (Ga. Ct. App. May 11, 2018), that a duty to safeguard personal information does *not* exist under Georgia common law. As the legislative and legal landscape continues to evolve in the data breach context, the question of whether a common law duty to safeguard personal information applies may likewise evolve in each of the 50 states.

In *McConnell*, Thomas McConnell filed a putative class action against the Georgia Department of Labor, asserting a negligence claim (among other claims) arising from the Department's improper disclosure of personal information of McConnell and the putative class members. According to McConnell, an employee of the Georgia Department of Labor, while acting within the scope of his official employment, sent an email to approximately 1,000 Georgians who had applied to the Department for services such as unemployment benefits. Attached to the email was a spreadsheet identifying the name, social security number, home phone number, email address, and age of over 4,000 Georgians (including McConnell) who had registered for Department services. Based on this conduct, McConnell alleged a claim for the negligent disclosure of personal information, seeking, as damages, out-of-pocket costs (for credit monitoring and identity protection services), damages arising from the adverse impact to credit scores, and damages for the "fear, upset, anxiety and injury to peace and happiness related to the disclosure of [his] personal identifying information, …" 2018 WL 2173252, at *1.

The trial court dismissed the negligence claim, ruling "there is no legal duty [under Georgia law] to safeguard personal information." *Id*. at *5. McConnell appealed this decision to the Georgia Court of Appeals. In a prior appellate decision in the same case (in 2016), the appellate court affirmed the trial court on the merits, explaining that Georgia's Legislature only imposed "notice" obligations after a data breach has occurred and had not imposed "any standard of conduct in implementing and maintaining data security practices." *McConnell v. Ga. Dep't of Labor* , 787 S.E.2d 794, 799 (Ga. Ct. App. 2016). But the

Georgia Supreme Court vacated that decision, ruling that the Court of Appeals first should have addressed the threshold issue of sovereign immunity before turning to the merits. *McConnell v. Ga. Dep't of Labor*, 805 S.E.2d 79 (Ga. 2017).

On remand, the Court of Appeals again addressed the merits, after ruling that McConnell's tort claims fell within Georgia's waiver of sovereign immunity in the Georgia Tort Claims Act. 814 S.E.2d 790, 2018 WL 2173252, at * 2-*4. On the merits issue, the Court of Appeals reiterated that duty is an essential element of any action for negligence, and that whether such a duty exists is a question of law. "The duty can arise either from a valid legislative enactment, that is, by statute, or be imposed by a common law principle recognized in the caselaw." *Id*. (quoting *Rasnick v. Krishna Hospitality, Inc.*, 713 S.E.2d 835, 837 (Ga. 2011)). McConnell argued that Georgia law recognized a common law duty "to safeguard and protect the personal information of another," citing Georgia's data breach notification statute and its Fair Business Practices Act. *Id*. at *6. But, according to the Georgia appellate court, neither statute gave rise to a common law duty.

Georgia's data breach notification statute, the Georgia Personal Identity Protection Act (OCGA §§ 10–1–910 through 10–1–915 (the "GPIPA")), did not give rise to a common law duty. The court ruled that, "despite the General Assembly's aspirational recognition of the harm caused by identity theft, the GPIPA does not proscribe any conduct in storing data or protecting data security. Rather the GPIPA proscribes particular conduct, that is, notification and the placement of a security freeze, only after a (known or suspected) data security breach has occurred. Because the GPIPA does not impose any standard of conduct in implementing and maintaining data security practices, we conclude that it cannot serve as the source of a general duty to safeguard personal information." 2018 WL 2173252, at *6.

Regarding Georgia's Fair Business Practices Act (the "FBPA"), that statute likewise did not give rise to a common law duty. The relevant part of the FBPA (O.C.G.A. § 10–1–393.8) provides that "a person, firm, or corporation shall not: ... [p]ublicly post or publicly display in any manner an individual's social security number." *Id*. But to "publicly post or publicly display" a social security number "means to intentionally communicate or otherwise make available to the general public[.]" *Id*. The *McConnell* court ruled: "Although the FBPA imposes a standard of conduct to refrain from intentionally and publicly posting or displaying SSNs, a legal duty to refrain from doing something intentionally is not equivalent to a duty to exercise a degree of care to avoid doing something unintentionally, which falls within the ambit of negligence." *Id.*

Accordingly, because the alleged legal duty – the duty to safeguard personal information – had no source in Georgia statutory authority or case-law, the appellate court affirmed the trial court, ruling that McConnell's negligence claim was properly dismissed for failure to state a claim upon which relief could be granted. *Id.*

Before *McConnell*, a federal court sitting in Georgia had predicted that Georgia would recognize a duty to safeguard personal information, flowing from the "general duty one owes to all of the world not to subject them to an unreasonable risk of harm." *In re The Home Depot, Inc. Customer Data Security*

Breach Litig, No. 1:14-md-2583-TWT, 2016 WL 2897520, at *3 (N.D. Ga. May 17, 2016). The 2016 *McConnell* decision refused to follow *Home Depot*, distinguishing the allegations in that case that the defendant had failed to address known security risks from the allegations in *McConnell* that the Department of Labor had made a purely unintentional error. 787 S.E.2d at 797 n.4. Although the 2018 *McConnell* decision did not address *Home Depot*, its affirmation of the core reasoning of the 2016 *McConnell* decision strongly undermines the legitimacy of the federal court's prediction of Georgia law.

Another federal district court relied on the 2016 *McConnell* decision to hold that *Home Depot*'s prediction of Georgia law should not be followed. *See Community Bank of Trenton v. Schnuck Markets, Inc.*, No. 15-cv-01125-MJR, 2017 WL 1551330, at *3 (S.D. Ill. May 1, 2017). That court also distinguished an earlier data breach case finding a duty to safeguard personal information as based on policies unique to Minnesota statutory law, including Minnesota's policy of sanctioning companies that fail to secure customer data. *Id.* (distinguishing *In re Target Corp. Data Sec. Breach Litigation*, 66 F. Supp. 3d 1154, 1312-13 (D. Minn. 2014)). And it discounted two Pennsylvania district court decisions finding such a duty, ruling that one was too old to be a reliable predictor for data breach cases and that the other had "no authoritative force whatsoever as a contested report and recommendation." *Id.* at *4 (discussing *Sovereign Bank v. BJ's Wholesale Club, Inc.* , 395 F. Supp. 2d 183 (M.D. Pa. 2005), and *First Choice Federal Credit Union v. The Wendy's Co.* , No. 2:16-cv-NBF-MPK (Doc 80) (W.D. Pa. Feb. 13, 2017)).

As discussed in a prior post, the Seventh Circuit affirmed the district court's decision in *Schnuck Markets*. [*Seventh Circuit: the economic loss doctrine precludes tort claims between participants in a contractual network that allocates risk for a data breach.*] Although the Court of Appeals primarily focused on the economic loss rule, it agreed the plaintiffs had not shown an actionable duty to safeguard personal information under either Illinois or Missouri law. *Community Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 816, 817-818 (7th Cir. 2018). Among other things, it noted that the only "consumer-facing mandate" statutorily imposed by either state was "notice" after discovery of a data breach, in contrast to the handful of states that had enacted statutes imposing a duty to safeguard personal information (such as Minnesota, Nevada, and Washington). *Id.* at 818.