Legal Opinion Letter

WLF Washington Legal Foundation

Advocate for freedom and justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302

Vol. 19 No. 1 January 16, 2009

PRIVACY & PERSONAL DATA SECURITY: THE NEXT LITIGATION FRONTIER?

by
Professor Raymond T. Nimmer

Widespread adoption of rules regarding security of personally identifiable information has been paralleled by a surge of class-action litigation against companies whose databases have been breached. They are a potential target beyond modern parallel. This setting potentially offers class action lawyers bountiful fuel. But courts and legislators should take a different path.

The fundamental policy issues require that we ask how much law should be given over to protect non-confidential, personal information and whether that law should be in a form of liability suits or non-litigation guidelines. Even if protection of non-confidential personal information is vital, laws grounded in rules not susceptible to high cost litigation and damage claims can better establish social expectations without causing a massive shift of value, largely to plaintiffs' lawyers.

There are two liability issues. The first is whether the holder of the data owes a duty to the person about whom the data relate in the absence of an express assumption of such duty. This "duty" issue can arise in tort or under implied warranty rules in contract law.

Either way, no implied obligation should exist. Most courts so hold. The traditional rule is that a person who properly obtains non-confidential data has a right to use it. The fact that I know your home address does not create a duty to keep that information secure. Indeed, such information is known by many people.

Some information is delivered under confidentiality restraints or is sufficiently sensitive that an implied duty can be inferred. But the presumption should be that data is free from legal constraints unless there are over-riding reasons to restrict its use, or impose liability for its disclosure. No general obligation of maintaining security should exist. If it were created, we would face an unwarranted restriction on ordinary discourse and information sharing, socially and commercially. While there are some benefits in reference to a sense of data security, these benefits do not over-ride the benefits of being able to use and deploy the information one knows without fear of a lawsuit.

The second issue is the "damages" issue. Even if a duty were created, no cause of action should exist if there are no proven, foreseeable damages cognizable under the particular cause of

---

Raymond T. Nimmer is the Dean and Leonard Childs Professor of Law at the University of Houston Law Center and co-director of the Houston Intellectual Property and Information Law Institute.Professor Nimmer maintains the *Contemporary Intellectual Property, Licensing & Information Law* blog (http://www.ipinfoblog.com/).

action chosen. The mere compromise of a database involving personally identifiable information does not necessarily lead to legally cognizable damages in the absence of a foreseeable and provable connection to actual harm to the data subject.

The damages most frequently asserted in security breach settings entails the *risk* that a wrong-doer may use the data for identity theft. But, while there have been numerous security breaches of identity theft incidents associated with those breaches has been very low. Thus, the litigation issue has been that, even if no identity theft occurred, is the distress and preventive actions caused by the risk of identity theft compensable. Most courts correctly hold that they are not.

In *Forbes v. Wells Fargo Bank*, 420 F. Supp. 2d 1018 (D. Minn. 2006), the court held that a bank was entitled to summary judgment on claims of negligence and breach of contract because the plaintiffs had no damages. There were no unauthorized transactions and plaintiffs could not recover damages for a risk of harm unless that risk resulted from a present injury, that is, "the threat of future harm, not yet realized, will not satisfy the damage requirement."

Similarly, in *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629 (7th Cir. 2007), the court was asked to decide whether Indiana law would allow individuals receiving notice of a security incident to recover their costs for credit monitoring or emotional distress. The Seventh Circuit said no. An Indiana statute imposed an obligation to provide notice in the event of a security breach but not liability:

> Had the Indiana legislature intended that a cause of action should be available against a database owner for failing to protect adequately personal information, we believe that it would have made some more definite statement of that intent. … The narrowness of the defined duties imposed, combined with state enforced penalties as the exclusive remedy, strongly suggest that Indiana law would not recognize the costs of credit monitoring that the plaintiffs seek to recover in this case as compensable damages.

The Seventh Circuit explained that plaintiffs had "not suffered a harm that the law is prepared to remedy. …"

Although, personal data security has become a burgeoning field in law, courts properly have shown a reluctance to impose an implied obligation to maintain the security of data of a non-confidential kind, regarding another party. A person rightfully in possession of such information has a right to use and disclose it – rights co-equal to the data subject. There is no actionable legal obligation to the other person, except for confidential or highly dangerous information.

ISBN 1056 3059