Lessons Learned From Recent Privacy Litigation*

by Kirk J. Nahra†

October 2007

Privacy and security litigation remains an area of intense interest. A wide variety of high-profile security breaches has focused attention on the risks associated with the use, disclosure and maintenance of personal information by entities in essentially all industries. New statutes continue to emerge, at both the state and federal level. Yet, there has been a relatively modest amount of privacy and security litigation, and no breakthrough decision has heralded a new era of litigation risks for companies that use and disclose personal information. What conclusions can we draw from the recent privacy and security litigation?

What Is the State of the Play Today?

- We know that there is an increasing awareness of privacy and security issues in litigation, even where a specific privacy law is not the focus of the case.
- The volume of privacy and security litigation has been relatively small, certainly much less than was predicted by many experts (including this one), although the amount of litigation is slowly growing.
- We are starting to see a wide range of cases based on security breaches or potential identity theft situations, although plaintiffs continue to face uphill struggles in these cases.
- And, while plaintiffs have become very clever at creating privacy and security causes of action, particularly in situations involving individual harm, courts—for the time being—remain relatively skeptical about many of these claims.

Key Lessons Learned

Within this framework, what are the major lessons learned from recent privacy and security cases?

---

* Reprinted from the October 2007 issue of *Privacy In Focus*®.

† Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, D.C., where he specializes in privacy and information security litigation and counseling for companies facing compliance obligations in these areas. He is the Chair of the firm's Privacy Practice. He serves on the Board of Directors of the International Association of Privacy Professionals, and edits IAPP's monthly newsletter, *Privacy Officers Advisor*. He is a Certified Information Privacy Professional. He can be reached at 202.719.7335 or knahra@wileyrein.com.

Damages Still Matter—A Lot

Judges—starting with a limited number of cases but now formulating a clear line of precedent—are imposing a significant hurdle for privacy and security cases, in that a failure to allege actual damages precludes proceeding with litigation. The first key case is also one of the most straightforward—*Smith v. Chase Manhattan Bank*, 741 N.Y.S.2d 100 (App. Div. 2002).

In *Smith*, a bank promised its customers that it did not and would not sell their personal information to third parties. Nevertheless, the suit alleged, the bank did sell customer lists to third parties, including a telemarketing firm. Moreover, the bank allegedly received a percentage of the proceeds from the products sold as a result of these telemarketing services.

Despite this egregious set of allegations, the court's decision is clear, and perhaps startling. The court dismissed the complaint, finding no allegations of actual damages. Instead, the court said that "the 'harm' at the heart of this purported class action is that class members were merely offered products and services, which they were free to decline. This does not qualify as actual harm." Moreover, "[t]he complaint does not allege a single instance where a named plaintiff or any class member suffered any actual harm due to the receipt of an unwanted telephone solicitation or a piece of junk mail." Accordingly, the court found that the complaint was appropriately dismissed for failure to state a cause of action. This means the court found that no legal claim existed on the facts as they were alleged, not that the allegations were incorrect.

Smith is the clearest enunciation of the "no damages" theory—but not the only one. More recent decisions (involving DSW and Acxiom Corp.), where potential identity theft had been alleged, followed the same idea—no actual damage, no case.

The court in *Forbes v. Wells Fargo Bank, N.A.*, 420 F. Supp. 2d 1018 (D. Minn. 2006), took this one step further, rejecting a claim by potentially harmed individuals against a bank, where the individuals had asserted negligence and breach of contract claims. This case involved a third-party service provider to a Wells Fargo subsidiary. The service provider was a victim of a theft, where computers containing unencrypted personal financial information were stolen. The bank notified these individuals about the theft; promptly, a class action suit was filed on behalf of the bank's customers. These plaintiffs asserted a variety of costs related to the theft, primarily to monitor their financial accounts against potential loss.

In line with other cases, the court rejected these claims, essentially because no evidence indicated that any information from these computers had been misused. The court also found that the personal time and money spent by this purported class "was not the result of any present injury, but rather the anticipation of future injury that has not materialized."

These cases now form a solid line of precedent. In *Randolph v. ING Life Ins. & Annuity Co.*, 486 F.Supp. 2d 1 (D.D.C. 2007), following the theft of a laptop, the court found that the plaintiffs had failed to allege any injury that is "actual or imminent, not conjectural or hypothetical." The court then concluded that "Plaintiffs' allegations therefore amount to mere speculation that at some unspecified point in the indefinite future, they will be victims of identity theft." Even more recently, in *Kahle v. Litton Loan Servicing LP*, 486 F.Supp. 2d 705 (S.D. Ohio 2007), the court, following a line of cases that "clearly reject the theory that a plaintiff is entitled to

reimbursement for credit monitoring services or for time and money spent monitoring her credit," found that any "injury of the plaintiff is purely speculative" and rejected the contention that this speculative injury could constitute damages in a negligence case.

The Seventh Circuit recently weighed in to the same effect. In *Pisciotta v. Old National Bankcorp*, 2007 WL 2389770 (7th Cir. Aug. 23, 2007), the US Court of Appeals, predicting the requirements of Indiana law, affirmed dismal of a proposed class action, stating that, "Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy."

A lack of actual damages—even in the face of clear security breaches—is now the primary hurdle in most privacy and security cases.

No Private Cause of Action—Don't Be Too Sure

While plaintiffs have struggled to assert private causes of action directly under privacy statutes such as HIPAA, they now are learning to be more creative—with the possibility that a new claim for "negligence" may emerge. The most likely candidate for leading precedent on this theory is the case of *Acosta v. Bynum*, 638 S.E.2d 246 (N.C. Ct. App. 2006). Here, the appellate court reinstated claims against a psychiatrist who allegedly allowed an office manager access to psychiatric records that were then used to cause harm to a patient. The appellate court found HIPAA created a standard of care plaintiffs might invoke in making claims that a defendant violated a standard of care. This decision therefore creates the opportunity for plaintiffs to use HIPAA as a measuring stick for a traditional tort claim—even where there was no obviously egregious behaviors assumed. While proof of damages will still be required, this case provides the plaintiff a means of circumventing the lack of a HIPAA cause of action. It is one to watch in the years ahead.

Acosta may be the clearest case on this "negligence" concept, but it is not the only recent case permitting "HIPAA like" claims to be brought without reliance on a HIPAA cause of action per se. While similar cases have not yet been brought based on other privacy statutes, this theory could work under numerous laws.

The recent case of *Sorensen v. Barbuto*, 143 P.3d 295 (Utah Ct. App. 2006), *cert. granted*, 150 P.3d 544 (Utah 2006), is also informative. In that case, a patient sued his former doctor for providing assistance to the defendant in a personal injury suit brought by the patient. While this case may be most noticeable for the idea that judges may seek out means of remedying violations when faced with a reasonably defined actual harm or particularly bad behavior, it presents an interesting spin on a HIPAA claim.

The *Sorensen* decision stems from Sorensen's suit against Barbuto (his former physician), brought after Sorensen learned of Barbuto's involvement with his opposing defense counsel. He asserted breach of contract and various tort claims against Barbuto, all of which were dismissed by the trial court. The Utah Court of Appeals reversed most of this dismissal.

The court first rejected Barbuto's claim that he violated no duty because Sorensen had placed his physical condition at issue in the case, finding that this "exception" to the physician-patient privilege doctrine could not be the basis for Barbuto to act against the patient in a suit where Barbuto was a

third party. The court then held that "ex parte communication between a physician and opposing counsel constitutes a breach of the physician's fiduciary duty of confidentiality." The court also held that the trial court's dismissal of Sorensen's negligence claim was in error, as the fiduciary duty that existed in this situation could support a negligence claim.

The court also found that Sorensen could pursue a claim for intentional infliction of emotional distress. Because Barbuto not only communicated ex parte with defense counsel, but also became a paid advocate for Sorensen's adversary, the conduct by Barbuto met the threshold of "extreme and outrageous" conduct necessary to sustain a claim for intentional infliction of emotional distress.

After full briefing, this case was argued before the Utah Supreme Court on September 7, so additional guidance may be forthcoming.

Herman v. Kratche, Case No. 86697, 2006 WL 3240680 (Ohio App. Dist. Nov. 9, 2006) is another case to watch. Here, the plaintiff received medical treatment from a clinic. The clinic sent the results of the treatment to the HR Department of the plaintiff's employer. The clinic was told by both the employer and the patient that there was no workers' compensation claim, and that nothing should be provided to the employer, yet the material continued to be sent to the employer. Herman alleged that she was "embarrassed, angry and emotionally distraught, and felt an ongoing anxiety about [her] privacy."

The court decision says that the clinic had a fiduciary duty to the patient and a duty to keep information confidential, and that it breached that duty. The fact that the employer also owed duties to the plaintiff didn't mitigate the clinic's breach. The court properly rejected the interesting idea that a HIPAA "circle of confidentiality"—a disclosure to another entity with HIPAA regulatory obligations—was not a violative disclosure. Accordingly, the court permitted various claims to go forward based on the unauthorized disclosure.

These cases are not uniform, but they do evidence a realistic possibility of two key theories being adopted—negligence, through a failure to meet a standard of care set by legislative or regulatory standards, and "breach of (fiduciary) duty," through failure to meet these same standards.

There Is No Class Action Breakthrough (Yet)

While these "quasi-negligence" cases present a real risk of becoming a new basis for privacy and security claims, these cases—so far—have focused on individual situations, where a specific individual faced a particular harm.

On a broader basis, there still has been no significant breakthrough case sustaining class action allegations. For example, even in the series of cases related to the ChoicePoint security breach—one of the most prominent breaches, and one where the facts led to development of state notification laws around the country—the class action plaintiffs have come up empty. In the most recent decision, *Harrington v. ChoicePoint Inc.*, CV 05-0124 MRP (C.D. Cal. Oct. 11, 2006), five separate actions were consolidated into a class action suit in the Central District of California, alleging violations of the Fair Credit Reporting Act and various California statutes.

The plaintiffs sought actual, statutory and exemplary damages, as well as injunctive relief, attorneys' fees and costs. The court rejected the FCRA claim because the plaintiffs failed to provide any evidence that would support their contention that the disclosed information met the three requirements of a "consumer report" under the FCRA. Once the federal claims were dismissed, the court declined to exercise supplemental jurisdiction and dismissed the state claims as well, resulting in a complete dismissal of all claims against ChoicePoint.

The question in these class action cases is whether any particular case will result in a breakthrough—and a resultant turnaround in—the attitudes of class action attorneys in these cases. The litigation against TJX presents this possibility—if the multiple cases that have been filed result in a substantial recovery. We also have seen recent class certifications—for settlement purposes only—in cases involving Commerce Bankcorp and American Express. While these settlements do not constitute formal precedent, and incorporate no court decisions altering the discussion on damages or the appropriateness of a class on the merits, they do warrant attention, because a sufficient number of class-oriented settlements may have the effect of altering the dynamics in these cases. That is, if defendants will pay, why not bring such suits?

The Plaintiffs Are Still Trying

For plaintiffs, the biggest potential opportunity has involved a substantial number of new cases filed in connection with an alleged breach of a single provision of the FACTA law, related to the "truncation" of credit card numbers on receipts provided to customers. These suits seek to use statutory minimum damages to evade the "no damages" issue. Thus, the plaintiffs' counsel have asserted "statutory damages" (because no actual damages exist), with claims totaling in the billions of dollars due to the large size of the proposed class. While these cases are only beginning, they present some real risks for defendants—and trivialize the actions of companies around the country to take better steps to protect the data they maintain. In these cases, clearly no one has been harmed; none of the cases (to my knowledge) even bothers to assert any actual harm. But they remain significant and an area for all companies to watch; they also should serve as a reminder to all companies that accept credit cards to make sure their practices fit this statutory standard.

The initial decisions are starting to trickle in, mostly from a single judicial district. One court rejected a motion to dismiss a FACTA class action, in *Leowardy v. Oakley Inc.*, No. 8:07-cv-0053, 2007 WL 1113984 (C.D. Cal. April 10, 2007), where the defense had asserted that the individuals had no standing to bring the suit under the private cause of action provisions of the statute. A similar standing decision was issued in *Eskandari v. IKEA U.S. Inc.*, No. 8-cv-01248, 2007 WL 845948 (C.D. Cal. March 12, 2007).

A potentially more significant decision was issued in *Spikings v. Cost Plus Inc.*, No. 2:06-cv-08125 (C.D. Cal. May 25, 2007). Here, the court rejected class certification in one of the FACTA cases in which plaintiffs alleged too much information was printed on card receipts. According to the court, "[i]n this case, if a class is certified and Plaintiff prevails, even the minimum statutory damages would be ruinous to Defendant.'' If the plaintiff was able to prove a willful violation, "statutory damages alone would range from a minimum of $340 million to a maximum of $3.4 billion.'' Focusing on the plaintiff's testimony that there had been no actual damages, the court also noted that "[m]ost importantly, denial of class certification in this case does not prevent any of Defendant's

customers who may have suffered actual damages as a result of Defendant's conduct from proceeding with individual cases to recover those damages.''

Don't Think That Privacy Laws Are a Good Shield From Discovery

Recent cases also make clear that most privacy laws do not create a barrier that can protect companies from the need to produce information in discovery. For example, the Mississippi Supreme Court in *Capital One Services, Inc. v. Page*, 942 So. 2d 760 (Miss. 2006), ordered a credit card issuer to turn over documents in a lawsuit brought by a cardholder, rejecting the card firm's claims that disclosure of the information is barred by federal G-L-B privacy provisions. Similarly, in *Ex parte National Western Life Insurance Co.*, 899 So. 2d 218 (Ala. 2004), the Alabama Supreme Court held that G-L-B does not shield the records of financial institutions' customers against disclosure to third parties pursuant to a discovery order in a private suit. Genuine litigation has been recognized as an appropriate means to cause the production of personal information, and, as long as the required procedures are followed, companies cannot use general privacy laws to prevent discovery.

Beware of State FOIA Claims

Perhaps similar to the discovery cases, companies (and individuals) need to be aware of the new risk that sensitive personal information may be subject to disclosure through government "open records" laws. For example, in *State ex rel. Cincinnati Enquirer v. Daniels*, 844 N.E. 2d 1181 (2006), the Ohio Supreme Court, in dicta, indicated that the state freedom of information laws trumped the HIPAA Privacy Rule, so that information held by the state, even where the state had a HIPAA-covered entity role, would be subject to disclosure under the Freedom of Information Act. A similar opinion was issued by the Attorney General in Texas, indicating that the open government law "requirements" indicated that HIPAA-protected data would be subject to disclosure. Companies and government entities should be re-evaluating their production processes or reconsidering exceptions to these laws, so that personal information is not disclosed inappropriately.

Conclusions

We know that privacy and security litigation is not going away. There is a continuing perfect storm consisting of new laws that have overlapping and potentially conflicting requirements, with increased enforcement and ongoing security breaches. Companies in all industries need to be aware of the risks of litigation and take steps to reduce those risks.

With that said, many uphill challenges remain to bringing successful privacy/security suits (or, conversely, lots of defenses still exist, even when companies have not behaved well). Damages are a substantial hurdle, particularly in class action cases. In "individual harm" situations, companies need to be careful to meet existing privacy and security standards, even where these standards contain no private right of action, as courts are beginning to recognize these standards as setting a standard of care that must be met under state law.

* * *