



COUGHLIN DUFFY LLP

ATTORNEYS AT LAW

***NEW TECHNOLOGIES AND THE PERILS  
THEY CREATE***

**Adam M. Smith, Esq.  
Timothy Moriarty, Esq.**

350 MOUNT KEMBLE AVENUE  
P.O. BOX 1917  
MORRISTOWN, NEW JERSEY 07962-1917  
PHONE: (973) 267-0058  
FACSIMILE: (973) 267-6442

WALL STREET PLAZA  
88 PINE STREET, 5TH FLOOR  
NEW YORK, NEW YORK 10005  
PHONE: (212) 483-0105  
FACSIMILE: (212) 480-3899

[WWW.COUGHLINDUFFY.COM](http://WWW.COUGHLINDUFFY.COM)

Copyright 2006 Coughlin Duffy, LLP. All rights reserved. This paper may not be reprinted or republished without the prior written permission of Coughlin Duffy, LLP.

Recent advances in technology have made “hi-tech” communication, publication and storage devices readily accessible to the smallest of businesses. The ability to communicate instantaneously, publish professional-looking materials at a desktop computer and store tremendous amounts of customer data has resulted in smaller businesses being able to compete with larger businesses. With the use of those technologies, smaller business can now operate more efficiently and profitably.

As much as this new technology has resulted in the predicted increased profitability, it has also created unforeseen potential liabilities for businesses, especially for small businesses that do not employ a professional risk manager. That lack of foresight has resulted in many companies leaving themselves unprotected (i.e. uninsured) against potential losses arising out of such new technologies as camera phones, the internet or the storage and portability of customer data. Recognizing and acknowledging the presence of those perils will enable a company to protect itself from losses that may arise from its use of that technology.

One of the most common devices utilized by businesses to safeguard against catastrophic losses is insurance. When addressing potential liabilities to third parties, the standard insurance product available is the comprehensive general liability policy. Such traditional insurance policies, however, were not and are not designed to protect against the risks presented by some of the new technologies. As a result, many businesses that rely solely on the comprehensive general liability policy will find themselves unprotected against the risks presented by many new technologies.

This paper will discuss certain technological advancements and the risks such advancements pose to businesses. It will also address the insurance coverage issues

presented by those risks under a comprehensive general liability policy and why businesses facing such liabilities may find themselves without insurance coverage needed to protect their assets.

## **I. THE RISKS POSED BY NEW TECHNOLOGY**

### **A. *Camera-enabled cell phones***

It does not require extensive economic research to recognize that almost everyone over the age of fifteen carries a cell phone. Moreover, one trip to the local wireless phone dealer is all that is necessary to understand that almost every new cell phone is equipped with a built-in digital camera. Employees and business invitees carrying around these miniature cameras expose many businesses to significant liabilities.

Gym locker rooms, clothing store changing rooms or restaurant bathrooms, all places where photographs of people changing or in embarrassing situations may be taken, expose their proprietors to liability for invasion of privacy claims. Any business that is entrusted with private, confidential and/or proprietary information is exposed to the risk of theft of that data. Although such a risk has always been present, it has exponentially increased given the ease of use of these devices and the ability to transmit the data. With just one click, a picture can be taken of sensitive information and sent electronically to thousands of people.

There are several potential types of claims to which businesses are exposed as a result of the usage of camera-enabled cell phones including, invasion of privacy; intentional or negligent infliction of emotional distress; negligent supervision of employees; or failure to maintain safe conditions for business invitees.

Recognizing the potential problems that camera-enabled cell phones can cause and the difficulty in distinguishing between a cell phone that can and cannot take a picture, local governments are increasingly passing ordinances and legislation to prohibit cell phone usage where the possibility of an invasion of privacy exists. *See*, “Hold It Right There, and Drop That Camera”, by Jo Napolitano, *The New York Times* (December 11, 2003.) Such ordinances will likely be subject to constitutional challenge given the difficulty in drawing the line as to where cell phone usage can and cannot be permitted. That being said, the federal government recently enacted the Video Voyeurism Protection Act of 2004, which provides that people have an expectation of privacy in places as public as a mall or a park.

**B.     *Storage of consumer data***

For years, large corporations have collected and stored a wide range of consumer information to assist in marketing and sales efforts. Many times the information involves sensitive personal and financial data of consumers. New technologies have dramatically decreased the cost of collecting that data and storing it electronically. It is essential that business organizations ensure that all company data is adequately protected with appropriate security and privacy policies. Because of the decreased cost of storage, the miniaturization of the memory devices and their ease of use, many smaller businesses are now utilizing the same tools of some larger companies in the gathering and storing consumer data. Those smaller businesses, however, may not have the financial wherewithal to handle the potential exposure to which the storage of such data exposes them or the resources to adequately protect that data.

Once a company compiles sensitive personal information about its customers, it has a responsibility to safeguard the information. Persons in possession of information about or property of “another person may in some circumstances have obligations to that person to safeguard its information or property. This creates a three-party security issue; in the event of intrusion or disclosure, it forces us to ask not only whether the intrusion was wrongful, but whether the stakeholder against who the intrusion occurred has liability to the third party because the stakeholder did not prevent the intrusion or disclosure.” Raymond T. Nimmer, *Chapter 8. Privacy and Data Protection Law, Part F. Private Data Systems*, Information Law § 8:91 (2005). Thus, “[t]o reduce the likelihood of identity theft and attendant liability, prudent businesses may wish to review and strengthen their data protection policies.” Peter F. Berk, *Practical Suggestions for Protecting Employee and Customer Electronic Data*, 12 NO. 7 Emp. L. Letter 1 (July, 2005).

There have been a multitude of recent data security breaches. For instance, Choice Point, Inc., experienced a security breach that affected more than 140,000 people in all fifty states. Mary J. Hildebrand and Jacqueline Klosek, *Recent Security Breaches Highlight the Important Role of Data Security in Privacy Compliance Programs*, 17 NO. 5 Intell. Prop. & Tech. L.J. 20 (2005). In addition, Bank of America reported that it lost computer data tapes containing personal and confidential information, including Social Security numbers and account information, of approximately 1.2 million federal employees. Jonathan Gould, *Congress Proposes Legislation Following Security Breaches by Choice Point and Bank of America*, 9 NO. 10 Elec. Banking L. & Com. Rep. 9 (2005). In 2005, CardSystems Solutions Inc. acknowledged that hackers obtained

information on 200,000 credit card and debit card accounts. DSW Shoe Warehouse suffered a database security breach in which hackers obtained 1.4 million credit card numbers and the names associated with those accounts.<sup>1</sup>

At least four consumer lawsuits were filed against ChoicePoint Inc., which admitted it accidentally sold personal data on 140,000 consumers to identity thieves. The suits have been consolidated in federal court and are requesting class action status, and seek monetary, statutory and punitive damages, including compensation for anxiety stemming from the fact that they may be a victim of identity theft. *Harrington v. Choicepoint*, No. 2:05-CV-01294-SJO-JWJ (C.D. Calif.). In addition, lawsuits or enforcement actions are pending against LexisNexis, Cardsystems Solutions, Inc, DSW, Inc., BJ Wholesale Club, Inc., U.S. Bancorp, and Eckerd Drugs.

BJ's agreed to settle Federal Trade Commission charges that it failed to implement adequate security measures to protect sensitive consumer information which constituted unfair business practices. The settlement requires BJ's to establish and maintain a comprehensive information security program. The settlement also requires BJ's to obtain an audit from a qualified, independent, third-party professional that its security program meets the standards of the order. According to BJ's SEC filings, as of May 2005, the amount of outstanding claims was approximately \$13 million. "BJ's has a \$16 million reserve to cover all costs related to the breach. DSW has set aside \$6.5 million and said costs could rise to \$9.5 million."<sup>2</sup> DSW agreed to settle Federal Trade Commission charges that its failure to take reasonable security measures to protect sensitive customer data was an unfair practice that violated federal law. Similar to the

---

<sup>1</sup> 1.4 million exposed in shoe data breach, available online at <http://msnbc.msn.com/id/7550562>.

<sup>2</sup> David Bank, Breaches of customers' data trigger lawsuits, (July 21, 2005), available online at <http://www.post-gazette.com/pg/05202/541454.stm>

settlement with BJ's, the "settlement will require DSW to implement a comprehensive information-security program and obtain audits by an independent third-party security professional every other year for 20 years."<sup>3</sup>

In addition, Eckerd has agreed to obtain express permission from customers before sending them marketing material on behalf of pharmaceutical companies. The policy change is part of a settlement agreement between the drugstore chain and the Florida attorney general's office, which investigated whether Eckerd breached customers' privacy and engaged in deceptive trade practices by sending unsolicited promotions. Eckerd will also contribute \$1 million to endow a chair in ethics at Florida A&M School of Pharmacy.

U.S. Bancorp settled a lawsuit brought by the Minnesota attorney general. U.S. Bancorp agreed to stop "the practice of sharing customer account information for the purposes of marketing non-financial products and services[.]"<sup>4</sup> In addition U.S. Bancorp agreed to contribute \$1.5 million to chapters of Habitat for Humanity in Minnesota, \$500,000 to the State of Minnesota, and \$1,034,000 to charitable organizations in other states in which the bank does business.<sup>5</sup>

A class action lawsuit has been filed by California credit card holders and merchants against Cardsystems Solutions, Inc. and others alleging a failure to maintain adequate data security which led to a security breach exposing over 40 million credit card holders to potential fraud. "The lawsuit alleges that Cardsystems Solutions, Merrick Bank, Visa and MasterCard have violated their duty to timely and properly inform

---

<sup>3</sup> *DSW Settles FTC Charges, Company Failed to Protect Sensitive Customer Data*, (December 5, 2005), available online at [http://www.consumeraffairs.com/news04/2005/ftc\\_dsw.html](http://www.consumeraffairs.com/news04/2005/ftc_dsw.html)

<sup>4</sup> *Minnesota Attorney General and U.S. Bancorp Settle Customer Privacy Suit*, available online at [http://www.ag.state.mn.us/consumer/Privacy/PR/pr\\_usbank\\_07011999.html](http://www.ag.state.mn.us/consumer/Privacy/PR/pr_usbank_07011999.html)

<sup>5</sup> *Ibid.*

consumers of the nature and degree of the alleged security breach. The suit claims that these violations constitute ‘unfair, unlawful and deceptive business practices’ under California's Unfair Competition Law.”<sup>6</sup> This lawsuit is still pending.

The potential costs of data security breaches may be astronomical, including the costs of: investigations, fines, court orders, injunctive relief, consumer litigation, vendor litigation, damaged business reputation, customer loss, loss of goodwill, shareholder suits, and internal investigation costs. *See* John F. Delaney, *Privacy, Data Security, and Outsourcing the Regulatory Framework*, 8444 PLI/Pat 611, 617 (October 24, 2005). What’s more, in light of recently enacted data notification laws, businesses may be required, at their own cost, to notify each and every individual whose information may have been lost.

#### 1. Data Notification Laws

California was the first state to enact legislation governing the disclosure and notification of data security breaches to affected consumers. Many states have followed suit, modeling their notification laws after California’s. In at least thirty-five states, legislation has been introduced or enacted regarding customer notification of security breaches that result in the unauthorized release of personal consumer information. Generally, the legislation requires companies “to notify consumers regarding breach of security in which certain personal information relating to those consumers was, or is reasonably believed to have been, acquired by an unauthorized person.” Thomas E. Scanlon, *Overview of Recent State Laws Requiring Notification of Security Breach*, 6

---

<sup>6</sup> *Cardsystems Named in Class Action Suit*, (June 30, 2005), available online at [http://www.consumeraffairs.com/news04/2005/cardsystems\\_suit.html](http://www.consumeraffairs.com/news04/2005/cardsystems_suit.html)

NO. 3 Privacy & Info. L. Rep. 6 (Nov. 2005) (citations omitted). Each states' data notification statute, however, is not identical, containing their own nuances.

## 2. Overview of California Security Breach Notification Law

California's Database Security Breach Notification Act, codified at Cal. Civ. Code § 1798.82 and § 1798.29, and General Security Standard for Businesses, codified at Cal. Civ. Code § 1798.81.5, require companies and government agencies that store personal information on California residents to implement safety procedures that safeguard data and disclose any breach of security to the individuals affected. Cal. Civ. Code § 1798.82 (a) affects any state agency, business, or person that conducts business in California and maintains computerized data that includes personal information. Cal. Civ. Code § 1798.82 (b) states that any breach of the security of the data must be reported in the most expedient manner following the discovery of the breach to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Cal. Civ. Code § 1798.82 (e) defines personal information as an individual's last name and first name or initial, in combination with a Social Security number; driver's license or California ID Card number; or account, debit card or credit card number, in combination with any security code, access code or password that would permit access to the account. Cal. Civ. Code § 1798.82 (g) provides that:

“[N]otice” may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.

(C) Notification to major statewide media.

Failure to promptly notify the information owner or licensee of the data makes the organization liable for civil damages. "The law allows any customer who is injured by a violation of [Cal. Civ. Code § 1798.82 ] to institute a civil action to recover damages." Francoise Gilbert, *Information Privacy and Security in California*, 1 NO. ABA SciTech Law. 8 (Fall, 2004). Thus, a company that fails to comply with the notification provisions of Cal. Civ. Code § 1798.82 may face legal action from both consumers and from the California Attorney General.

On the other hand, the General Security Standard for Businesses, Cal. Civ. Code § 1798.81.5, requires that businesses owning or licensing such personal information about a California resident, when held in unencrypted form, implement and maintain reasonable security procedures and practices to protect the personal information from unauthorized access, use, modification, destruction, or disclosure. California's Database Security Breach Notification Act and General Security Standard for Businesses should have a significant impact on business practices with respect to the protection of electronic data gathered and stored because of the potential for severe penalties. These penalties can be inflicted through class action lawsuits and other penalties and fines that may be levied against the organization for negligence in exercising an inadequate standard of care in

protecting the information. In addition, companies face possible additional costs attributable to security breaches, including damage to image, reputation and brand resulting from public awareness of and perception of security breaches, the cost of notifying data owners, and the cost of defending lawsuits brought against the company.

### 3. Florida's Data Notification Statute

Florida passed H.B. 481, Fla. Stat. Ann. § 817.568 *et seq.*, effective July 1, 2005. Fla. Stat. Ann. § 817.5681(1)(a) provides that “[a] person who conducts business in this state and maintains computerized data in a system that includes personal information provide notice of any breach of the security of the system, following a determination of the breach, to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person.” There exists a forty-five day grace period for notification after the security breach. Fla. Stat. Ann. § 817.5681(b)1 states that if notification to consumers is not performed within this time period, fines of up to \$1000 per day for up to thirty days can be imposed. Pursuant to Fla. Stat. Ann. § 817.5681(b)1, if the company does not notify the customers of the breach after the subsequent thirty day period, the fines increase to \$50,000 for each thirty day period, up to 180 days. If notification is not made within 225 days, any person required to make notification under Fla. Stat. Ann. § 817.5681(b)2 who fails to do so is subject to an administrative fine of \$500,000. Pursuant to Fla. Stat. Ann. § 817.5681(10)(b), fines of up to \$50,000 are specified for failure to document the breach, or for failure to keep records of the breach for up to five years.

Most of the state notification laws track the California or Florida notification statutes by generally defining "personal information" as an individual's name, plus any one or

more of the following "data elements:" the individual's Social Security number, driver's license or state identification card number, or account number in combination with a password or other access code for the account, when either the name or the data elements are not encrypted. However, some of the state notification laws apply to a broader range of information. Therefore, companies looking to comply with the consumer notification laws on a nationwide basis could consider increasing security measures for all data elements that any of the states include in the definition of "personal information" to the extent they retain such data elements.

#### 4. Federal Legislation

A series of high-profile data breaches in the first half of 2005 prompted lawmakers to introduce more than a half-dozen bills that would require companies to notify consumers affected by security breaches.<sup>7</sup> "Some of the bills have exceptions for encrypted data, and some require companies to report breaches only when they determine there's significant risk to customers."<sup>8</sup> Many companies are lobbying for federal legislation that would preempt state data breach notification laws to create a more uniform system. This sentiment was echoed in a recent article where one journalist in discussing state data notification statutes wrote, "[a] 'patchwork quilt' of state laws, as some critics have called the multiple laws, has caused some large businesses and trade groups to call for a national law that preempts state laws."<sup>9</sup> Federal legislation dealing with data breach notification has been introduced in both the House of Representatives and in the Senate.

---

<sup>7</sup> David Bank, *Breaches of customers' data trigger lawsuits*, The Wall Street Journal (July 21, 2005).

<sup>8</sup> Grant Gross, *2006 in Congress: 'Full plate' for tech, telecom*, (December 27, 2005) available online at <http://www.itnetcentral.com/article.asp?id=15395&leveli=0&info=home>.

<sup>9</sup> Grant Gross, *Data breach bills unlikely to pass before 2006*, (November 11, 2005), available online at [http://www.infoworld.com/article/05/11/11/HNdatabreachbill\\_1.html](http://www.infoworld.com/article/05/11/11/HNdatabreachbill_1.html).

Recently, “[a] bipartisan group of senators ... introduced legislation to create a national data privacy law that would require businesses and other organizations to disclose data breaches that result in the loss of consumers' personal information.”<sup>10</sup> The main objectives of the bill are:

1. Greater protection of and control over the use of key personal data such as Social Security numbers and financial account information;
2. Increased penalties for breaches and facilitating identity theft; and
3. A nationwide standard for notifying consumers when their personal information has been breached.<sup>11</sup>

While those bills remain pending before Congress, certain legislation has already been enacted requiring certain business to properly protect consumer/client data. The Federal Financial Modernization Act, commonly know as Gramm-Leach-Bliley Act (“GLBA”), 15 U.S.C. § 6801 *et seq.*, was passed by Congress and signed by President Clinton November, 1999. The GLBA states, “[i]t is the policy of Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those consumers’ non-public information.” 15 U.S.C. § 6801. Section 501(b) GLBA mandates that financial institutions develop and implement administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. Put simply, it requires financial institutions to prevent unauthorized access to non-public, personal

---

<sup>10</sup> Brian Krebs, *Data Breaches Spur Congressional Action, Federal Notification Law Would Trump State Measures*, (July 18, 2005), available online at <http://www.washingtonpost.com/wp-dyn/content/article/2005/07/18/AR2005071800613.html>.

<sup>11</sup> Jeanne Sahadi, *Breaches: Federal law on the way? Lawmakers have proposed several bills that seek to better protect personal data*, (July 7, 2005), available online at [http://money.cnn.com/2005/07/06/pf/security\\_bills/](http://money.cnn.com/2005/07/06/pf/security_bills/).

information. The Health Insurance Portability and Accountability Act , 42 U.S.C. § 1320(d) *et seq.*, and The Sarbanes-Oxley Act of 2002, 15 U.S.C. § 7201 *et seq.*, also mandate that electronically stored consumer/client information be adequately protected.

## **II. INSURANCE COVERAGE FOR NEW TECHNOLOGIES UNDER A TYPICAL COMPREHENSIVE GENERAL LIABILITY POLICY**

A business exposed to risks from new technologies, whether through the collection and storage of legislatively-protected consumer data, camera-enabled cell phones or through its use of the internet, faces significant financial uncertainty if its sole protection against third party liability is the comprehensive general liability (“CGL”) insurance policy. Traditionally, CGL policies provide cover for “property damage” or “bodily injury”. Losses arising from new technologies, however, will likely not fit within those definitions.

More recent versions of the CGL policy provide cover for “personal injury” and “advertising injury”. That cover, however, will often be excluded if the underwriter believes that the policyholder presents an “e-commerce” risk. Even where not excluded wholesale, the cover provided by a CGL policy for “personal injury” and “advertising injury” as it relates to new technology claims is suspect. For example, although an invasion of privacy claim is customarily covered under the “personal injury” section of a CGL policy, many policies will require a publication or utterance before granting cover for such a claim. Or, to fall under the “advertising injury” section, there must be a nexus between the policyholder’s advertising activities and the offending activity. Quite simply, the gaps in cover are clear.

It is beyond the scope of this paper to address each and every issue raised by the different potential claims that could arise out of a “new technology” claim. To highlight

some issues, we discuss the insurance coverage issues potentially implicated in a claim arising out of a camera-enabled cell phone or a data breach.

**A. *Camera-enabled cell phones***

Given the newness of the technology, there are no reported decisions addressing coverage under a CGL policy for a claim arising out of the use of a camera-enabled cell phone. An analogy is easily drawn, however, to claims arising out a hidden, fiber optic camera in a changing room at a photography studio.

In that case, decided under Mississippi state law, American Guarantee and Liability Insurance Company (“American Guarantee”) sought a declaratory judgment that the CGL policy it issued to Hattiesburg Coca-Cola Bottling Company (“Hattiesburg Coke”) provided no coverage or duty to defend for twenty-one lawsuits, each from a different claimant. *American Guarantee and Liab. Ins. Co. v. 1906 Co.*, 273 F.3d 605, 607 (5<sup>th</sup> Cir. 2001). The complaints alleged that “the insured’s male employee had surreptitiously videotaped female customers changing clothes in a women’s dressing room on the insured’s premises.” *Ibid.* The plaintiffs alleged invasion of privacy, outrage, intentional infliction of emotional distress, fraud, negligence and exploitation of minors. *Id.* at 609.

The facts of that case are worth noting. The voyeur at issue’s father was the CEO of Hattiesburg Coke. With his son developing an interest in photography, the CEO authorized the use of Hattiesburg Coke funds to open a photography studio for him to operate. Although the studio was located at a separate site, it was owned and operated as a division of Hattiesburg Coke. Unbeknownst to the photography studio’s clients, the voyeur was surreptitiously videotaping them undressing in the dressing room with a

hidden fiber optic camera. Lawsuits were filed against the voyeur, the CEO of Hattiesburg Coke, the photography studio and Hattiesburg Coke itself.

The District Court determined that the insurer had no duty to defend or indemnify Hattiesburg Coke, Hattiesburg Coke's CEO or the voyeur under either Coverage A (the bodily injury and property damage section) or Coverage B (the personal injury or advertising injury section) of the CGL policy. *Id.* at 607-08. The District Court concluded that the voyeur's actions were not within the scope of his employment and "that the injuries alleged by the women did not constitute an 'occurrence' under the policy because they were intended or expected from the standpoint of the insured." *Id.* at 609.

On appeal, a Fifth Circuit reversed and granted motions for summary judgment against American Guarantee. *Ibid.* The Court of Appeals differentiated "personal injury" from "bodily injury." *Id.* at 612. The Court of Appeals explained "unlike Coverage A, which excludes coverage for [b]odily injury or property damage expected or intended from the standpoint of the insured, Coverage B expressly extends coverage to liability for personal injury ... other than bodily injury, caused by certain defined offenses arising out of the insured's business." *Ibid.* (Citations and quotations omitted). Therefore, the Court of Appeals concluded that the triggering act under Coverage B may be caused by an intentional act. *Ibid.*

In particular, the CGL insurance policy issued to the insureds stated:

- a. We will pay those sums that the insured becomes legally obligated to pay as damages because of "personal injury" or "advertising injury" to which this insurance applies...we

will have the right and duty to defend any "suit" seeking those damages

b. This insurance applies to "personal injury" only if caused by an offense:

(1) Committed in the "coverage territory" during the policy period; and

(2) Arising out of the conduct of your business...

10. "Personal injury" means injury, other than "bodily injury," arising out of one or more of the following offenses:

c. Wrongful eviction from, wrongful entry into, or invasion of the right of private occupancy of the room, dwelling or premises that a person occupies by or on behalf of its owner, landlord or lessor.

The Fifth Circuit noted that the "invasion of private right of occupancy" phrase is not defined in the policy and had not been interpreted by Mississippi courts. *Id.* at 618. Mississippi law recognizes the tort of invasion of privacy and requires that commercial property owners protect their business invitees from unreasonable risks of harm while visiting their premises. Accordingly, the court reasoned that the Mississippi Supreme Court would find that the voyeur, by secretly videotaping young women in the business' dressing room, invaded their "right to private occupancy" of that room. *Id.* at 619. At best, the court noted that the phrase "invasion of the right of private occupancy" is ambiguous as a matter of law. *Id.* at 620. Because of this ambiguity, the Fifth Circuit concluded that the clause should be construed in favor of coverage in the present case. *Id.*

Pursuant to the policy issued to Hattiesburg Coke, under Coverage B American Guarantee agreed to "pay those sums that the insured becomes obligated to pay as damages because of personal injury ... to which this insurance applies." *Id.* at 612

(internal quotations omitted). The policy defined “Personal injury” as “injury, other than ‘bodily injury’, arising out of one or more of the following offenses....” *Ibid.* “Under Coverage B, American Guarantee agreed to indemnify Hattiesburg Coke and Richard Thomson for non-bodily personal injury liability caused by an offense ‘arising out of the conduct of’ the insureds’ business.” *Id.* at 616. The Court of Appeals determined that Hattiesburg Coke and the CEO could be held liable for damages for non-bodily personal injury to the plaintiffs. *Ibid.* Additionally, the Court of Appeals concluded that the facts alleged in the underlying complaints were caused by offenses which arose out of the conduct of Hattiesburg Coke’s business. *Id.* at 616-17. Accordingly, the Court of Appeals determined that American Guarantee was obligated to defend and indemnify Hattiesburg Coke and the CEO in the underlying lawsuits filed by the women. *Id.* at 620.

The court found three viable causes of action against Hattiesburg Coke and the CEO: (1) failure to maintain reasonably safe conditions for business invitees; (2) negligent hiring (of the CEO’s voyeuristic son); and (3) negligent entrustment of the photography equipment. Moreover, in analyzing whether the alleged conduct fell within the definition of “personal injury” under the policy, the court concluded that in light of the control exerted by Hattiesburg Coke over the photography studio, the voyeur’s offenses arose out of the conduct of Hattiesburg Coke’s business.

Although coverage was found in that particular circumstance, the peculiar set of facts present in *1906 Co.* will be difficult to replicate. Applying the analysis to a case arising out of the use of a camera-enabled cell phone, it is unlikely that such a phone will be bought and supplied by the company. Even if the phone is supplied by the company, it is likely supplied as a communication device, not to take photographs. Thus, it will be

difficult to conclude that in such circumstances the offense arose out of the insured's business.

**B. *Storage of consumer data***

As with any other claim, insurance coverage for data security breaches depends on the allegations contained in the complaint. When the claim arises out the loss of electronically stored consumer data, many coverage issues under a CGL policy will likely result. For example, many of the recent actions alleging the loss of electronically stored consumer data have been filed by governmental entities. Such claims may seek only the imposition fines or penalties, damages which are not commonly recoverable under CGL policies.

One question that arises is whether damage or loss of electronic data is “property damage” as defined under a CGL policy. Most CGL policies provide cover only for tangible property damage. In most states, a standard CGL policy does not provide coverage for intangible property loss. *Guelich v. American Protection Ins. Co.*, 772 P.2d 536 (Wash. Ct. App. 1989); *Columbia Nat. Ins. v. Pacesetter Homes, Inc.*, 532 N.W.2d 1, 6 (Neb. 1995). The prevailing view is that electronic data is not tangible property damage that is covered under a CGL policy. *See, Lucker Mfg. v. Home Ins. Co.*, 23 F.3d 808, 818 (3<sup>rd</sup> Cir. 1994) (“Tangible property is property that can be felt or touched, or property capable of being possessed or realized.”); Paul M. Yost, *et al.*, *In Search of Coverage in Cyberspace: Why the Commercial General Liability Policy Fails to Insure Lost or Corrupted Data*, 54 SMU L.Rev. 2055, 2066-68 (2001); *See also, State Auto Prop. and Cas. Ins. Co. v. Midwest Computers & More*, 147 F. Supp.2d 1113, 1116

(W.D. Okl. 2001) (“[C]omputer data cannot be touched, held, or sensed by the human mind; it has no physical substance. It is not tangible property.”)

However, at least one court has held that loss of electronic data is tangible property damage. *See Computer Corner, Inc. v. Fireman’s Fund Ins. Co.*, 46 P.3d 1264 (N.M. 2002). In that case, Computer Corner, Inc. engaged in the sale and service of personal computers. Fireman’s Fund Insurance Company (“Fireman’s”) issued a CGL policy to Computer Corner, Inc. *Id.* at 1265. A customer brought his computer to Computer Corner, Inc. because an error message was displayed on his computer screen. *Ibid.* The customer informed an employee that various important files were on the computer and were not backed up. *Id.* at 1266. The technician that repaired the customer’s computer reformatted the hard drive and therefore the customer was unable to “access the data stored on his hard drive.” *Ibid.* As a result, the files were lost and permanently destroyed. *Ibid.* The court determined that loss of the pre-existing electronic data constituted tangible property damage. *Id.* at 1268-71. Thus, the court ruled that Fireman’s had a duty to indemnify Computer Corner, Inc. under the CGL policy. *Id.* at 1270.

In addition, the standard form CGL policy was amended in 2004 to ensure that there is no ambiguity on the issue of whether electronic data is property damage and whether such policies provide cover for such damage. The 2004 CGL policy has amended the definition of “property damage” to state that “electronic data is not tangible property.” Moreover, the 2004 CGL policy specifically excludes coverage for the loss of electronic data. These amendments to the CGL policy should make clear to

policyholders that insurers do not intend to provide cover for losses of electronically stored data.

### **III. CONCLUSION**

New technologies are providing opportunities for smaller companies to compete with larger ones. Those technologies, however, present new liability risks that smaller businesses may not have the resources to assume. It is imperative that these companies review their insurance portfolios to ensure that coverage exists should they become exposed to a loss.

When reviewing their CGL policies with respect to a particular claim or exposure, businesses should consider the following issues:

#### Coverage A: Bodily Injury and Property Damage

- Is intangible property damage covered?
- Is electronic data tangible property damage?
- Was the injury expected or intended from the standpoint of the insured?

#### Coverage B: Personal and Advertising Injury

- Does the offense arise out of the insured's business?
- Was there a publication or utterance?
- Was there a nexus to the insured's advertising activities?
- Has this cover been excluded due to the nature of the insured's business?

In short, CGL policies were not designed with claims arising out of new technologies in mind. Policyholders seeking cover under CGL policies for these types of claims should expect resistance from their insurers in granting cover.