

INSURING PRIVACY: IS YOUR COMPANY COVERED?

Matthew J. Schlesinger and Jason M. Silverman

I. INTRODUCTION

Privacy is emerging as one of the hottest cyber-tort liability issues of the new millennium. Common law, as well as various statutes and regulations, have protected the right to privacy for years. But with the proliferation of Internet use, the public has become keenly aware of the ease with which private information can be obtained and disseminated in the e-commerce age. As a result, federal and state governments have enacted new laws that create additional potential liability for companies that transact business through the Internet, and several parties have instituted a number of high-profile breach-of-privacy lawsuits in the past few years.

In this era of increasing risk, many companies who engage in e-commerce have recognized the potential importance of insurance coverage for privacy claims or lawsuits. Traditional comprehensive general liability¹ policies, the most common type of business insurance, as well as new specialized Internet policies, may provide coverage for privacy claims. But the wording of particular policies is critical, and coverage disputes in this relatively untested area are likely. After briefly setting forth the most common types of privacy-related liabilities that companies face today, this article examines the potential for coverage for privacy claims and the possible battle lines along which insurers and insureds may face off as liabilities are incurred and claims are made.

II. LIABILITY FOR PRIVACY VIOLATIONS

Breach-of-privacy suits can stem from common law, as well as federal and state statutes. Under common law, privacy torts generally include the fol-

1. Hereinafter CGL.

Matthew J. Schlesinger is a partner and Jason M. Silverman is an associate in the Washington, D.C., office of McKenna Long & Aldridge L.L.P.

lowing: (1) unreasonable intrusion upon the seclusion of another; (2) appropriation of another person's name or likeness; (3) unreasonable publicity given to another's private life; and (4) portrayal of an individual in a false light.² At the federal level, various laws exist that protect privacy rights online. This legislation includes the Electronic Communications Privacy Act (prohibiting unauthorized access to computers);³ the Wiretap Act (prohibiting the interception of data as well as knowing disclosure of such illegally obtained data);⁴ the Children's Online Privacy Protection Act (regulating the gathering of information from children);⁵ and the Gramm-Leach-Bliley Act (regulating the collection and distribution of personal and financial information by "financial institutions," including banks and insurers).⁶

A new significant bill concerning online privacy was introduced in the Senate on April 18, 2002, by Sen. Ernest Hollings (D.-S.C.).⁷ This bill would require website operators and Internet service providers to obtain consent from customers or users before collecting and disclosing certain types of information. The type of consent to be obtained would depend upon the degree of sensitivity of the information. Companies transacting business through the Internet would have to obtain *affirmative* consent from a consumer before collecting "sensitive personally identifiable information" from that person. "Sensitive personally identifiable information" includes race, political party affiliation, religious beliefs, sexual orientation, Social Security number, and certain financial information. For other kinds of less sensitive information (including, for example, name, e-mail address, and telephone number), Internet companies would be required to provide consumers "robust notice" and an opportunity to "opt out of," or decline consent. A private right of action would be granted to consumers to pursue

2. RESTATEMENT (SECOND) OF TORTS §§ 652A-652E (1977).

3. 18 U.S.C. §§ 2701-2711 (2000) (hereinafter ECPA). In addition to forbidding unauthorized access to computers, the ECPA also contains a prohibition against intentionally "[exceeding] an authorization to access" a "facility through which an electronic communication service is provided." Under the section of this statute granting a private civil right of action against violators, 18 U.S.C. § 2707 (2000), plaintiffs have alleged that the placement and subsequent access of "cookies" by an Internet site on a user's computer constitutes such unauthorized access. *In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1277 (C.D. Cal. 2001).

4. 18 U.S.C. §§ 2510-2522 (2000). Like the ECPA, the Wiretap Act also authorizes a private civil right of action. 18 U.S.C. § 2520 (2000).

5. 15 U.S.C. §§ 6501-6506 (2000). The statute regulates the collection of "personal information," such as the child's first and last name, home address, e-mail address, telephone number, and Social Security number. The Federal Trade Commission may add other categories of information as well. 15 U.S.C. § 6501 (2000).

6. 15 U.S.C. §§ 6801-6809 (2000). The Gramm-Leach-Bliley Act restricts release by financial institutions specifically of "nonpublic personal information" to third parties unaffiliated with the financial institution. "Nonpublic personal information" is defined as "personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution." 15 U.S.C. § 6809 (2000).

7. Online Personal Privacy Protection Act, S. 2201, 107th Cong. (2002).

alleged violations.⁸ Several major high-tech firms have voiced opposition to this proposed legislative scheme,⁹ and, if passed in its current form, this bill would present additional privacy liability exposure to companies doing business on the Internet.

Further, the government appears to be stepping up its privacy enforcement activity. The chairman of the Federal Trade Commission recently stated, "I think there is a great deal we can do under existing laws to protect consumer privacy. . . . At this time, we need more law enforcement, not more laws," and "[w]e will increase our enforcement of laws protecting consumer privacy."¹⁰ In addition to governmental enforcement of privacy laws, claims are also being asserted against companies by private individuals, alleging violations of federal and state privacy laws.¹¹

Companies can expose themselves, often inadvertently, in numerous ways to the application of a myriad of privacy laws and regulations. Recently, for example, Eli Lilly & Company, manufacturer of Prozac, mistakenly released, through e-mail, the e-mail addresses of 669 people who had registered for Lilly's e-mail medication reminder service.¹² Also, domain-name registrar Network Solutions, Inc., is reported to have forwarded to some of its customers the private e-mails of other customers sent to Network Solutions' support department requesting help.¹³ In this Internet age, protecting private information has indeed become a daunting task for most companies.

III. HOW MANY TYPES OF PRIVACY CLAIMS ARE COVERED UNDER STANDARD CGL POLICIES?

CGL policies provide coverage for defense costs and liabilities resulting from injury or damage to third parties allegedly caused by the insured. These policies typically cover four categories of liability: property damage, bodily injury, personal injury, and advertising injury. Invasion of privacy

8. *Id.*

9. Andy Sullivan, *High-Tech Firms Criticize Online Privacy Bill* (Apr. 25, 2002), available at <http://reuters.com/news/article.jhtml?type=technologynews&storyID=883562>.

10. Remarks of Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond*, The Privacy 2001 Conference, Cleveland, Ohio (Oct. 4, 2001), available at <http://www.ftc.gov/speeches/muris/privisp1002.htm>; see also Thomas M. Regan & Matthew F. Henry, *Federal Trade Commission—Loosening the Reins on Online Privacy*, MEALEY'S LITIGATION REPORT: CYBER TECH & E-COMMERCE 35-43 (Apr. 2002).

11. See, e.g., *In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272 (C.D. Cal. 2001); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *Crowley v. CyberSource, Inc.*, 166 F. Supp. 2d 1263 (N.D. Cal. 2001) (Wiretap Act, *supra* note 4, and ECPA, *supra* note 3, among others).

12. See *Eli Lilly Settles FTC Charges Concerning Security Breach* (Jan. 18, 2002), available at <http://www.ftc.gov/opa/2002/01/elililly.htm>.

13. Robert Lemos, *NSI Customers Report Privacy Breach* (June 20, 2001), available at <http://news.com.com/2100-1001-268781.html?legacy=cnet>.

has been covered under CGL policies for some time under the personal and advertising injury coverage grants. Typically, CGL policies provide coverage for “injury arising out of . . . [o]ral or written publication of material that violates a person’s right of privacy.”

Relatively few cases discuss coverage under CGL policies for invasion-of-privacy claims. Of those decided, most arise in the context of various types of actions brought by employees against employers. Courts have found coverage for alleged privacy violations where, as examples, an employee was singled out for a drug test,¹⁴ and an employer threatened to disclose private information about an employee.¹⁵

In a case decided earlier this year, *St. Paul Guardian Insurance Co. v. Centrum GS, Ltd.*,¹⁶ an employer that terminated an employee subsequently posted “wanted posters” with the former employee’s picture, name, home address, and driver’s license, automobile tag, and Social Security numbers. The poster implored anyone who saw the former employee to call security. The insurance company argued that the former employee’s breach-of-privacy claim was not covered because the privacy violation did not stem from the “business activity” of the insured, a building owner/manager. The Fifth Circuit disagreed. Noting the insured’s responsibility for protecting the building and the safety of its tenants, the court found as follows:

In light of the potential duty and perceived risk, Appellants posted information concerning a perceived risk to the Centrum Building and its tenants in a place where it could be viewed and appropriately used. Giving the term “business activity” its plain meaning, Appellants’ actions were consistent with their business of owning and managing property.¹⁷

In one nonemployment case, *St. Paul Fire & Marine Insurance Co. v. Green Tree Financial Corp.*,¹⁸ liability for harassing telephone calls made by a debt collection agency that were said by the court to “offend a reasonable person of ordinary sensibilities” was found to trigger CGL coverage. The calls were allegedly “rude and abusive” and occurred over the course of an eight-year period.¹⁹ The insurance policy covered personal injury arising out of “written or spoken material made public which violates an individual’s right of privacy.”²⁰ The insurer argued “that it was not obligated to defend [the insured] because the claimants’ pleadings did not specifically allege an offense covered by the personal injury terms of its policies,” such as invasion of privacy.²¹

14. *Ellis v. Transcontinental Ins. Co.*, 619 So. 2d 1130 (La. Ct. App. 1993).

15. *Great Am. Ins. Co. v. Hartford Ins. Co.*, 621 N.E.2d 796 (Ohio Ct. App. 1993).

16. 283 F.3d 709 (5th Cir. 2002).

17. *Id.* at 714.

18. 249 F.3d 389 (5th Cir. 2001).

19. *Id.* at 394.

20. *Id.* at 393.

21. *Id.* at 394.

The court, however, found the allegations to trigger the insurer's duty to defend because "the factual allegations in [the] case clearly [supported] a cause of action for invasion of privacy under Texas law."²²

IV. POSSIBLE CGL POLICY BATTLEGROUNDS FOR POLICYHOLDERS AND INSURERS ON PRIVACY CLAIMS

A. *The "Publication" Requirement*

In the context of the Internet, the scope of privacy coverage in most CGL policies may be argued by insurers to be limited in at least two ways that could leave some e-commerce companies unprotected. First, CGL policies typically require a privacy violation to be based on an "oral or written *publication* of material." The word "publication" is undefined in CGL policies, and courts may find themselves grappling with the term's proper interpretation in the Internet age. Internet privacy "violations," for example, can often involve the sale or dissemination of private information to a discreet set of businesses or organizations, as opposed to the public at large. Does sending e-mails containing private information to a limited number of people constitute a "publication of material"?²³

Outside the insurance context, some courts construe "publication" to include utterances to just one other person, or perhaps to a few. For example, in *Ratts v. Board of County Commissioners*,²⁴ the court construed the "publication" element of the tort of "false light publicity" simply as "publication of some kind to a third party." Few courts, however, have interpreted the term "publication" as it relates to coverage for privacy claims. In one recent insurance case, however, the court indicated that, while "*telling* members of the local community" private facts could arguably constitute "public disclosure," making disclosure of such facts to an individual lender did not constitute "giving publicity."²⁵

Further, although decided under language slightly different from that in the standard CGL form, the Fifth Circuit decision in *Green Tree* suggests that not all courts will construe the "publication" requirement to preclude coverage even for underlying invasion-of-privacy torts for which "publi-

22. *Id.* at 394–95.

23. *See supra* notes 12 and 13.

24. 141 F. Supp. 2d 1289, 1324 (D. Kan. 2001). *But see* L&D of Oregon, Inc. v. Am. States Ins. Co., 14 P.3d 617, 620 (Or. Ct. App. 2000) ("To constitute an actionable invasion of privacy, a disclosure of private facts must be public in the sense that it was communicated 'either to the public generally or to a large number of persons as distinguished from one individual or a few.'" (citation omitted)).

25. *Marleau v. Truck Ins. Exch.*, 37 P.3d 148, 153–54 (Or. 2001) (emphasis added). Ultimately, the court found that there was no coverage under the personal injury provision of the insurance policy.

ation” is not an essential element.²⁶ In that case, the insurance policy covered “written or spoken material *made public* which violates an individual’s right of privacy,”²⁷ as opposed to the “[o]ral or written *publication* of material that violates a person’s right of privacy.” Still, the court found coverage for the placement of harassing phone calls—not necessarily the “making public” or publication of private information—because such activity supported a cause of action for breach of privacy under Texas law.²⁸

Another reason that the term “publication” should not be limited to the broad dissemination of information may be found in the definition of “advertisement,” first found in the 1998 CGL form. In an attempt to preclude coverage for advertising injury resulting from individual sales calls, “advertisement” is defined in the 1998 form as advertising activity involving the broad dissemination of information: “Advertisement’ means a notice that is broadcast or published to the general public or specific market segments about goods, products, or services for the purpose of attracting customers or supporters.” Had insurers wanted to limit the term “publication” in the same manner, they could have done so by amending the appropriate policy language.

At the very least, privacy claims involving the misuse of image and likeness on a web page or some other broad electronic dissemination of private information should meet the “publication” requirement. But companies should be aware that insurers may argue that actions that precede publication, such as the improper “gathering” and use of information about a person, are insufficient to constitute a covered CGL privacy claim. Furthermore, unless the term “publication” is construed to encompass the dissemination of information to individuals or small groups, policyholders may be deprived of coverage for a host of privacy offenses not dependent upon the broad dissemination of private information.

B. *The “Advertising, Broadcasting, Publishing or Telecasting” Exclusion*

A second potential hurdle for e-commerce companies that seek coverage for privacy claims is the CGL policy exclusion that precludes advertising and personal injury coverage for insureds in the business of “advertising, broadcasting, publishing or telecasting.”²⁹ Advertisers and broadcasters must typically purchase separate insurance, often referred to as media cov-

26. See *St. Paul Fire & Marine Ins. Co. v. Green Tree Fin. Corp.*, 249 F.3d 389 (5th Cir. 2001).

27. *Id.* at 393 (emphasis added).

28. *Id.* at 394.

29. Before 1998, the standard CGL form excluded coverage for “[a]dvertising injury arising out of . . . [a]n offense committed by an insured whose business is advertising, broadcasting, publishing or telecasting.” In 1998 the exclusion was expanded to include all privacy offenses by such insureds, not just those committed in the course of “advertising,” as before.

erage, for such exposures. But courts have not yet provided guidance with regard to whether any company with a website could be construed to be an excluded “advertiser.”

A company that utilizes its website as little more than an extension of its own brochures and advertisements probably will not be subject to the “advertiser” exclusion. However, as most users of the Internet are aware, the advertising conducted on the websites of companies that do not consider themselves to be “advertisers” or “broadcasters” can be extensive. The banner or pop-up advertisements that appear on many websites are an obvious example. Further, many companies with websites use “cookies” to track online behavior and target advertisements using the information gained.³⁰ Hence, under the 1998 and earlier CGL forms (currently in widespread use), insurers could argue that a business with a website that displays banner ads, tracks user behavior for marketing purposes, or even includes some “entertainment” component is an excluded advertiser, broadcaster, or publisher, potentially leaving a broad range of companies that transact business over the Internet with no CGL privacy claim protection at all.

Support for the position that the “advertiser” exclusion should be construed narrowly to preclude personal and advertising injury coverage only for true “advertisers, broadcasters, publishers or telecasters” can be found in *American Employers’ Insurance Co. v. DeLorme Publication Co., Inc.*³¹ The policy at issue in *DeLorme* contained a typical advertiser exclusion, excluding coverage for advertising injury “arising out of . . . [a]n offense committed by an insured whose business is advertising, broadcasting, publishing or telecasting.”³² The court, construing the language of the exclusion “according to its plain and commonly accepted meaning,” held that the exclusion applied to “insureds whose primary, essential, chief or principal business is publishing.”³³ Although the court found the exclusion to apply, it did so only because the insured was, in fact, a “publisher,” its essential business being the publishing of maps.

Interestingly, too, a new CGL form, published in 2001, should alleviate policyholders’ concerns about whether the operation of a website, or even conducting limited “advertising,” could preclude them from having personal or advertising injury coverage under their CGL policies. In the new form, the “advertiser exclusion” is renamed as “Insureds in Media and Internet Type Businesses” and has been broadened to exclude website designers and Internet service providers. But with respect to other types of e-commerce companies, the new form also states that “the placing of

30. See, e.g., Theodore Grossman & Aaron Grossman, *Lifting the Veil on Internet Privacy*, MEALEY’S CYBER TECH LITIG. REP. (Sept. 2000).

31. 39 F. Supp. 2d 64 (D. Me. 1999).

32. *Id.* at 72.

33. *Id.* at 81.

frames, borders or links, or advertising, for you or others anywhere on the Internet, is not by itself, considered the business of advertising, broadcasting, publishing or telecasting.”³⁴ Further, the definition of “advertisement” has been modified to specifically include for purposes of advertising injury coverage “material placed on the Internet or on similar electronic means of communication.” Also, “that part of a web-site that is about your goods, products or services for the purposes of attracting customers or supporters is considered an advertisement” that is covered.³⁵ Accordingly, the new form clarifies that most companies whose core business is not advertising but who simply use their websites to advertise should not be subject to the “advertiser” exclusion.

V. PRIVACY COVERAGE UNDER THE NEW E-COMMERCE INSURANCE FORMS

Unfortunately for policyholders, insurers are under pressure from reinsurers to “control or exclude e-commerce risks from general liability policies.”³⁶ At the same time, insurers are marketing a number of new policy forms specifically touted as providing coverage for e-commerce risks.³⁷ The specialized policies are attractive to insurers because such policies permit insurers to “rate exposures separately rather than give blanket coverage for a single premium.”³⁸ From the perspective of the policyholder, among other things, these policies specifically cover web-based activities, removing any doubt that may exist about coverage for such activities under CGL policies. But the e-commerce policies are not standardized and can vary widely from insurer to insurer. Also, as such policies are new, they are relatively untested in the courts. Accordingly, the true scope of coverage provided by the new cyber-liability policies is still less than clear.

Many of the new policies, however, provide some type of coverage for privacy claims. Also, importantly, the “publication” of private information

34. The exclusion of personal and advertising injury in the new form specifically precludes coverage not only for those whose business is “advertising, broadcasting, publishing or telecasting,” but also for those whose business is “[d]esigning or determining content of web-sites for others; or [a]n Internet search, access, content or service provider.”

35. “Advertisement” is defined in the new form differently from how it was defined in the 1998 form in two important respects: “Advertisement” means a notice that is broadcast or published to the general public or specific market segments about your goods, products or services for the purpose of attracting customers or supporters. For the purposes of this definition: (a) Notices that are published include material placed on the Internet or on similar electronic means of communication; and (b) Regarding web-sites, only that part of a web-site that is about your goods, products or services for the purposes of attracting customers or supporters is considered an advertisement.”

36. Paul D. Winston & Gavin Souter, *Losses May Prompt Restrictions on Terms, Conditions*, *Bus. Ins.*, Sept. 24, 2001.

37. *Id.*

38. *Id.*

is not required for privacy coverage under some new Internet forms. For example, one insurer covers simply “infringement of any right to privacy or of publicity,” while policies sold by another are triggered by “any form of invasion, infringement, or interference with right of privacy. . . .” Thus, Internet privacy claims based upon, for example, the intrusion upon seclusion, which may not require disclosure of information, may be covered under some of the new policies. In fact, certain policies sold by insurers specifically include “intrusion” as a wrongful act that is covered.

But, as noted, not all e-commerce policies provide the same scope of coverage. At least one policy defines covered “Internet Activities” as the display or transmission of matter through the Internet, or dissemination of matter by other means as may be shown in the declarations of a particular policy. Although the policy does not extend so far as to require “publication,” on its face such a policy may allow the insurer to argue that privacy risks associated with the mere collection of private data are not covered. This situation also exists with respect to another insurer’s media liability policy. Under this policy, coverage for privacy violations hinges on “making known to any person” the offending material.

Companies that do business on or through the Internet must also be aware of certain other conditions and exclusions that insurers could use to dramatically reduce the scope of coverage for privacy claims under the new Internet policies. First, the policies typically exclude claims arising from government actions, including regulatory enforcement actions.³⁹ For example, an Internet liability policy form excludes “claims or loss against you that is brought by or on behalf of the Federal Trade Commission (FTC), Federal Communications Commission (FCC) or any other federal state or local government agency or ASCAP, SESAC, BMI or other licensing organizations in such entity’s regulatory, quasi-regulatory or official capacity, functions or duties. . . .”

The government action exclusion could prove particularly limiting as federal and state authorities expand their activities in connection with on-line privacy issues. The Children’s Online Privacy Protection Act⁴⁰ permits enforcement by either the Federal Trade Commission or state attorneys general. The Gramm-Leach-Bliley Act may be enforced by a number of federal agencies depending upon the type of financial institution involved, including the Federal Trade Commission, the Securities and Exchange Commission, and the Boards of Governors of the Federal Reserve System

39. In addition to this government action exclusion, most Internet policies, like most CGL policies, exclude coverage for liability arising out of criminal acts. Because the Wiretap Act, *supra* note 4, and the ECPA, *supra* note 3, are criminal statutes, coverage for liability arising out of a violation of these laws may be excluded by most policies.

40. 15 U.S.C. § 6504 (2000).

or of the Federal Deposit Insurance Corporation.⁴¹ In the past few years, the Federal Trade Commission and certain state attorneys general have pursued a number of enforcement actions against companies—Toysmart.com is one example—for collecting and using personal information about consumers.⁴² The number of cases is likely to increase significantly as enforcement becomes more vigorous.

Also, at least one major insurer excludes coverage for privacy claims arising out of the “intentional violation of [a company’s] privacy policy.” In the face of consumer concerns and new requirements, and perhaps in an effort to ward off further regulation, many companies publish a privacy statement that includes the company’s policy on collecting and sharing private information. The privacy statement itself, however, may create legal liability as it easily can be construed to be a binding promise. It is not difficult for companies to fall out of compliance with their privacy statements.

In fact, the chairman of the Federal Trade Commission has indicated that enforcement of online privacy policies is a priority of the commission.⁴³ A number of the private and governmental Internet privacy cases filed concern the alleged violation of posted privacy policies.⁴⁴ Policyholders, accordingly, must be prepared to confront the insurer argument that any violation of a privacy statement that results in a claim is “intentional” and is, therefore, not covered, necessarily resulting in a fact-intensive and potentially expensive coverage dispute.

Finally, although not necessarily considered an “exclusion,” e-commerce companies must be cognizant of the scope of the territorial provision in their policies. At least one insurer’s policies apply “anywhere,” but only so long as the underlying suit is filed in the “United States of America, its territories or possessions, Canada or Puerto Rico.” Privacy standards are arguably stricter in Europe, and U.S.-based companies have been subject to enforcement actions or suits in foreign countries. Accordingly, when purchasing a cyber-liability policy, a policyholder must consider not only the location where alleged wrongful acts may occur but also the jurisdictions in which the company may face suits.

41. 15 U.S.C. § 6805 (2000).

42. See First Amended Complaint for Permanent Injunction and Other Equitable Relief, *FTC v. Toysmart.com LLC*, No. 00–11341-RGS (D. Mass., filed July 10, 2000), available at <http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm>.

43. Remarks of Muris, *supra* note 10.

44. One allegation in the Federal Trade Commission complaint filed against Toysmart.com was that the company had represented in its privacy policy that it would not “disclose, sell, or offer for sale” the personal information voluntarily submitted to it by customers, but offered its customer lists for sale anyway when faced with bankruptcy. *Toysmart.com LLC*, No. 00–11341-RGS. See also *Crowley v. CyberSource, Inc.*, 166 F. Supp. 2d 1263 (N.D. Cal. 2001).

VI. CONCLUSION

The facts of each individual claim and the numerous terms and conditions of the applicable policy must be examined for a full assessment of the potential for coverage for any claim. But as privacy regulations and litigation increase, companies must understand the scope of the privacy coverage afforded both by their traditional policies and by the new Internet policies on the market. One thing is sure: there will be more privacy claims, and there will be coverage disputes over which claims are covered and which are not. Policyholders that know their policies and their rights are likely to fare the best.

