MEALEY'S™
Emerging Insurance Disputes

How To Maintain A 'Sterling' Reputation With Your Clients: What You Need To Know About CGL Coverage For Unauthorized Recording Claims

by
Colin B. Willmott
and
Jonathan L. Schwartz

Goldberg Segalla LLP

A commentary article reprinted from the February 5, 2015 issue of Mealey's Emerging Insurance Disputes

LexisNexis®

Commentary

How To Maintain A 'Sterling' Reputation With Your Clients: What You Need To Know About CGL Coverage For Unauthorized Recording Claims

By
Colin B. Willmott
and
Jonathan L. Schwartz

[Editor's Note: Colin B. Willmott is an associate in the Global Insurance Services Practice Group of Goldberg Segalla LLP. He focuses his practice on general liability and insurance coverage matters involving commercial general liability policies. Jonathan L. Schwartz is a partner in the Global Insurance Services Practice Group of Goldberg Segalla LLP. He concentrates his practice on insurance coverage litigation and counseling, including primary and excess commercial general liability, professional liability/errors and omissions, commercial auto, employer's liability, employment practices liability, and directors and officers liability insurance policies. Any commentary or opinions do not reflect the opinions of Goldberg Segalla or LexisNexis, Mealey's. *Responses are welcome.]*

One of the most remarkable and memorable scandals of 2014 involved Donald Sterling, the longtime owner of the Los Angeles Clippers, who received a lifetime ban from the National Basketball Association.[1] What triggered this scandal? A bigotry-laced audio recording was unearthed, which purported to be a private conversation between Sterling and his girlfriend V. Stiviano. Sterling's actions were widely deplored, yet a not insignificant minority of commentators expressed concern over punishing a man for comments he made allegedly in the privacy of his own home. These concerns are not limited to Mr. Sterling's situation, as recent rapid technological advances cause this privacy concern to become magnified. Nearly everyone has a recording device in the form of a smartphone. The ability to surreptitiously post what was intended to be a private conversation has never been easier.

This battle between the right to privacy and the monitoring and recording of private communication is at the center of the proliferation of class action lawsuits. *See e.g.*, Robert Milligan & Joshua Salinas, *California Invasion of Privacy Act Cases on the Rise*, Law360, June 2, 2014 ("If a company records or monitors inbound or outbound telephone calls with customers or employees, it runs the risk of violating California's call recording and monitoring laws, which have become enticing to the plaintiff's consumer class action bar."); Michael Mallow & Christine Reilly, *Recording Cellphone Calls in California Is Risky for Companies*, Law360, May 15, 2014 ("The lure to plaintiffs' firms is evident, given the potential for enormous class action damages and the relatively low barrier to pleading . . . violations [of the applicable California Penal Code sections]."). A representative sample of these class action lawsuits resulting from the alleged unauthorized recording of conversation is *McCabe v. Six Continents Hotels, Inc.*, which is pending in the United States District Court for the Northern District of California, No. 3:12-CV-04818-NC. That class action lawsuit alleges that Six Continents Hotels monitored and recorded the putative class members' phone calls to a hotel reservation hotline, without their consent, in violation of California Penal Code § 632.7.[2]

These unauthorized recording class action lawsuits[3] are, or should be, on the proverbial radar of insurance

carriers that write commercial general liability ("CGL") policies. Policyholders are turning in increasing numbers to their policies' "personal and advertising injury" coverage when confronted with these claims. In particular, policyholders contend that the offense of "oral or written publication, in any manner, of material that violates a person's right of privacy" (the "Privacy Offense") provides coverage. The jurisprudence regarding whether unauthorized recording claims satisfy the Privacy Offense is nuanced, complex, and divisive. Whether coverage applies to an unauthorized recording claim generally comes down to two questions: 1) does the claim satisfy the "publication" requirement in the Privacy Offense, and if so, 2) which exclusions, if any, bar coverage?

This article focuses on the answers to these two questions and provides practical claim handling suggestions for carriers confronted with these thorny claims.

I. What Statutory Relief Is Available For Consumers And Employees Subject To Unauthorized Recordings?

To address the rising concern over electronic surveillance, federal and state governments have enacted laws to regulate the interception of private communications. In 1986, the federal government enacted the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 *et seq.*, which prohibits the interception and disclosure of wire, oral, or electronic communications. The ECPA allows for recovery in the form of equitable or declaratory relief, actual or statutory damages (whichever is greater between $100 a day per violation, or $10,000), punitive damages, attorney's fees and other litigation costs. 18 U.S.C. § 2520.

Also, 48 states, as well as the District of Columbia, have a statute either prohibiting the interception of communications and imposing criminal liability, creating a private right of action, or both. While some statutes cover wire, oral, and electronic forms of communication, some cover only one form of communication. *See* https://www.fas.org/sgp/crs/misc/R41733.pdf. Nonetheless, virtually all of the statutes that create a private right of action allow the award of statutory damages, which, in the aggregate, can amount to multi-million dollar exposure for businesses and their insurers. *E.g.*, CAL. PENAL § 637.2 ($5,000 per violation); OHIO REV. CODE ANN. § 2933.65 (whichever is greater between $200 per day for each day of violation, or $10,000); WIS. STAT. § 968.31 (whichever is the greater between $100 per day for each day of violation, or $1,000).

II. How Have Courts Decided The 'Publication' Requirement In Unauthorized Recording Cases?

As referenced above, policyholders are seeking CGL coverage for these unauthorized recording class action lawsuits. They are specifically targeting the Privacy Offense. In virtually all of these coverage disputes, a fundamental issue is whether the Privacy Offense's publication requirement is satisfied.[4] Accordingly, this section will focus on the jurisprudence examining the "publication" requirement as applied to unauthorized recording claims.

Cases Finding The Requirement Satisfied In The Surveillance Context

In *Bowyer v. Hi-Lad, Inc.*, 216 W. Va. 634, 609 S.E.2d 895 (2004), the Supreme Court of Appeals of West Virginia articulated an unusually broad interpretation of the term "publication." In doing so, the Supreme Court determined that the subject CGL policy provided coverage to a hotel owner who allegedly subjected a hotel employee to oral surveillance, in violation of West Virginia's Wiretapping and Electronic Surveillance Act ("WESA"). The CGL policy issued by Westfield Insurance Company ("Westfield"), the hotel's insurer, contained standard Privacy Offense language. The lower court had determined that the publication requirement was not satisfied. The Supreme Court of Appeals disagreed. The Supreme Court of Appeals found significant that the term "publication" was undefined in the Westfield policy and dismissed Westfield's argument that the term "publication" required publication to third parties as in defamation cases. Nonetheless, the Supreme Court of Appeals concluded that even if a transmission to a third-party was needed, the surveillance system functioned in a way that anyone in the office where the surveillance monitoring equipment was placed had the ability to listen to the employee's conversations.

Similarly, in *National Fire Insurance Co. of Hartford v. NWM-Oklahoma, LLC, Inc.*, 546 F. Supp. 2d 1238, 1241 (W.D. Okla. 2008), an Oklahoma federal district court concluded that the Privacy Offense's "publication" requirement was met because the insured allegedly had the ability to listen to private conversations

via a baby monitoring system. Without specifically deciding whether "publication" required dissemination of information to a third party, the district court found compelling that the baby monitoring system enabled third parties, including the insured's customers, to listen to private conversations. The district court also suggested that if the insured's employees could listen in on the private conversations, the "publication" requirement could be satisfied, at least for purposes of the duty to defend.

Another district court concluded that dissemination of private information to the public at large was not required to satisfy the "publication" requirement in the Privacy Offense. In *Encore Receivable Mgmt., Inc., v. Ace Property & Cas. Ins. Co.*, 2013 U.S. Dist. LEXIS 93513 (S.D. Ohio Jul. 3, 2013),[5] two underlying lawsuits alleged that the insured operated a call center where the employees were recording telephone conversations between customers and customer service representatives without obtaining the customer's consent, in violation of California Penal Code § 637.2. The insurers maintained that for there to be a "publication," there needed to be distribution of the information or news to the public. The district court rejected that argument and instead held that "publication" occurs once a conversation is transmitted to a recording device. The district court explained, "this Court need not find that the communications were actually disseminated to third parties, because the initial dissemination of the conversation constitutes a publication at the very moment that the conversation is disseminated or transmitted to the recording device." Nonetheless, the district court found that there was evidence that the recordings were disseminated to the public, in light of the allegations that the recorded communications "were listened to and eavesdropped on" and were disclosed to employees of the companies for which the insured operated the call center.

The reasoning in *Bowyer* and *Encore* leaves insurers in a precarious position. These courts' explanation of the alleged multiple meanings of "publication" effectively affords the Privacy Offense an awkward and untenable construction. This explanation begs the question, how can there be more than one reasonable interpretation of "publication" when, like in the defamation context, the injury to the plaintiff occurs only after third parties learn of the claimant's private or secret information?

Cases Finding The Requirement Not Satisfied In The Electronic Surveillance Context

In *Defender Security Co. v. First Mercury Insurance Co.*, No. 1:13-cv-00245-SEB-DKL, 2014 U.S. Dist. LEXIS 33318 (S.D. Ind. Mar. 14, 2014), the district court correctly found that First Mercury Insurance Company ("First Mercury") did not have a duty to defend Defender Security Company ("Defender Security") in connection with telephonic communications with certain employees, representatives, and agents that were recorded without their consent, in violation of California Penal Code § 632. Focusing on the term "publication," the district court found significant that Defender Security maintained a record of the call, but did not relay the private conversation to anyone. Further, the district court found compelling that any personal information disclosed by the claimant to the insured was, in fact, disclosed by the claimant, herself, not by the insured. Notably, the district court expressly disagreed with *Encore*.

In sum, many jurisdictions have not yet addressed this issue directly. It thus remains to be seen how broadly or narrowly other courts will construe the "publication" requirement in the Privacy Offense. The district court's reasoning in *Defender Security* is the most in line with common sense. Not only does it incorporate the ordinary meaning of the word "publication," but it also ensures that the provision in the insurance policy actually means something and is not simply a throwaway requirement.

III. How Have Other States Analyzed The 'Publication' Requirement In Analogous Situations?

In addition to unauthorized recording claims, the "publication" requirement in the Privacy Offense plays a significant role in other contexts, including claims made under the Fair and Accurate Credit Transactions Act ("FACTA"), under the Telephone Consumer Protection Act ("TCPA"), the Fair Credit Reporting Act ("FCRA"), under state statutes prohibiting the dissemination of consumers' ZIP codes, and in the aftermath of data breaches. It may be quite helpful to see how courts construe the "publication" requirement in other circumstances because, due to the dearth of cases directly addressing "publication" in the surveillance context, the application of the term in other settings may offer clues as to how a specific jurisdiction will answer the question in the context of unauthorized recording claims.

FACTA Claims

Courts have analyzed the "publication" requirement in situations involving the Fair and Accurate Credit Transactions Act (FACTA) 15 U.S.C. § 1681 *et seq*. FACTA was designed to reduce identity theft by, for example, regulating how credit card information is handled and requiring fraud alerts. In particular, businesses have been sued under the "truncation of credit card and debit card numbers" provision. These businesses have, in turn, sought coverage under the Privacy Offense. In *Creative Hospitality Ventures, Inc. v. U.S. Liability Insurance Co.*, 444 Fed. App'x 370 (11th Cir. 2011), a putative class sued a restaurant for printing credit card receipts that contained more than the last five digits of the customer's credit card number and/or the credit card's expiration date. In response to the lawsuit, ETL requested that its insurer defend and indemnify it. The pertinent question in the subsequent coverage litigation was whether the term "publication" included a merchant providing a customer with a receipt during a retail transaction that informed the customer of his/her own credit card number and expiration date. The Eleventh Circuit determined that since ETL did not broadcast or disseminate the credit card information to the general public, the "publication" requirement was not satisfied.

In another FACTA case, *Ticknor v. Rouse's Enterprises, LLC*, Case No. 12-1151, 2014 U.S. Dist. LEXIS 21129 (E.D. La. Feb. 20, 2014), the plaintiffs argued that the term "publication" should be defined broadly to include "printing." The plaintiffs further argued that "publication" did not require disclosure of information to a third party. The district court dismissed those arguments and determined that "for there to be 'publication' under the 'personal and advertising' provision of the Evanston insurance policy, the material must be made generally known, announced publicly, disseminated to the public, or released for distribution." The court found the analysis in *Creative Hospitality* instructive and, therefore, concluded that providing a customer with a contemporaneous record of a retail transaction did not involve any dissemination to the public.

In sum, the reasoning from the FACTA cases should be instructive for surveillance cases where the claimant's phone conversation is recorded only for internal purposes, such as training of employees, but not broadcasted to outside entities. But even so, analogizing FACTA cases to surveillance cases may prove difficult when the recorded conversations are disseminated to a third party or to the general public.

ZIP Code Claims

Several state statutes, including California's Song-Beverly Act, prohibit a business from requiring as a condition to accepting credit cards as payment that the cardholder provide personal identification information. CAL. CIV. § 1790 *et seq.* California courts have determined that personal identification information includes information like a cardholder's address (which includes his/her ZIP Code) and telephone number. Massachusetts has a similar statute that has been construed to apply to requests for a customer's ZIP code. MASS. GEN. LAWS ch. 93, § 105(a).

A few recent cases have discussed the "publication" requirement in the context of ZIP code claims. For instance, in *OneBeacon America Insurance Co. v. Urban Outfitters, Inc.*, 21 F. Supp. 3d 426 (E.D. Pa. 2014), the underlying plaintiffs asserted violations of various statutes prohibiting companies from requesting ZIP code information for promotion and marketing purposes. In considering the "publication" requirement, the district court reviewed the meaning of "publication" under Pennsylvania law; noted that words in insurance policies must be construed according to their natural, plain, and ordinary meaning; examined several dictionary entries for "publication"; and concluded that "promulgation to the public, even to a limited number of people, is the essence of publication." Since there was no allegation of public dissemination of the information, the district court deemed the "publication" requirement not satisfied.[6]

Courts in need of guidance in determining the meaning of "publication" in the unauthorized recording context can look to *OneBeacon*. The district court there correctly identified that the "publication" analysis is a fact-intensive one and should be geared toward whether information was alleged to have been disseminated to a third party. Inquiries in the electronic surveillance context, especially where a company records caller conversations, are likewise fact-dependent. In sum, application of the "publication" requirement in surveillance cases can be straightforward—simply recording conversations should not trigger the "publication" requirement, whereas disseminating those conversations to a third party should satisfy the requirement.

TCPA Claims

A statutory scheme that policyholders have argued as instructive in the surveillance context is the TCPA. The TCPA is a wide ranging statute that prohibits, among other acts, the sending of unsolicited advertisements by fax or text message. 47 U.S.C. § 227. Courts have directly addressed the "publication" requirement in the context of alleged TCPA violations. For instance, in *Valley Forge Insurance Co. v. Swiderski Electronics, Inc.*, 223 Ill. 2d 352, 860 N.E.2d 307 (2006), the underlying plaintiffs sued Swiderski Electronics for allegedly sending unsolicited facsimiles advertisements in violation of the TCPA. The Illinois Supreme Court agreed that there was a "publication" of material because "Swiderski published the advertisements both in the general sense of communicating information to the public and in the sense of distributing copies of the advertisement to the public." Notably, the Illinois Supreme Court followed Black's Law Dictionary's definitions of "publication" as "communication to the public" and "the act of or process of issuing copies for general distribution to the public."

While some courts addressing coverage for TCPA claims have concluded that the term "publication" requires a public dissemination, other courts conclude that "publication" in the TCPA context does not require that the material be communicated to a third-party. *See, e.g.*, *Park Univ. Enters. v. Am. Cas. Co.*, 442 F.3d 1239, 1250 (10th Cir. 2006); *W. Rim Inv. Advisors, Inc. v. Gulf Ins. Co.*, 269 F. Supp. 2d 836, 847 (N.D. Tex. 2003).

Insurers should be wary when relying on TCPA cases because there are substantial differences between the TCPA and unauthorized recording statutes with regard to the interests of the parties. For example, the TCPA purportedly protects individuals from the violation of their seclusion rights by unsolicited advertisements, whereas plaintiffs in surveillance cases are worried that their secrecy rights are being violated by the disclosure of their personal conversations. These are distinctly different interests which may dissuade a court from finding the two contexts analogous. Nevertheless, a court may be persuaded by how courts have interpreted "publication" in the TCPA context, regardless of the underlying factual and equitable circumstances.

FCRA Claims

In arguing that electronic surveillance or unauthorized recording claims satisfy the "publication" requirement in the Privacy Offense, policyholders are likely to point to how courts have decided the "publication" requirement in actions involving the Fair Credit Reporting Act ("FCRA"). 12 U.S.C. § 1681 *et seq*. Among other protections, the FCRA prohibits the unauthorized disclosure of consumer credit information. In *Zurich American Insurance Co. v. Fieldstone Mortgage Co.*, 2007 U.S. Dist. LEXIS 81570 (D. Md. Oct. 27, 2008), the underlying plaintiff alleged that a mortgage company improperly accessed his credit information in formulating prescreened offers in order to prepare mortgage refinancing solicitations. With regard to the "publication" question, the court insisted that the ordinary and customary meaning of the word should apply since it was not defined in the policy. Therefore, the court, relying on a line of TCPA cases, reasoned that "publication" could easily be understood to "encompass the printing and mailing of written solicitations." In a case with similar facts in the Northern District of Illinois, the court relied on *Swiderski, supra*, for the proposition that "publication" can constitute "communication to as few as one person. . . ." *Pietras v. Sentry Ins. Co.*, No. 06 C 3576, 2007 U.S. Dist. LEXIS 16015, at *10 (N.D. Ill. Mar. 6, 2007).

Like with TCPA claims, FCRA claims are not truly analogous to electronic surveillance claims. For FCRA claims, the insured allegedly accessed customers' credit information without their consent and then sent customers individualized prescreened offers. There is no dissemination of information to third parties in FCRA actions, since the claimants' credit information is merely shown to the claimant, herself. Further, in FCRA actions, the insured has improperly accessed the claimants' secret information, whereas in unauthorized recording claims, the claimant has freely shared her secret information (albeit without knowing that the conversations are being recorded).

Data Breach Claims

Similar to the explosion in litigation surrounding unauthorized recordings or surveillance, data breaches are occurring on a massive scale. In dealing with data breach situations, courts have also reviewed the "publication" requirement. In a low-tech data breach where computer tapes fell out of the back of a van, the court determined that since no facts indicated that the computer files were accessed by anyone and caused no harm, the court was unable to infer that there had been "publication." *Recall Total Info. Mgmt., Inc. v.*

Fed. Ins., 147 Conn. App. 450, 83 A.3d 664 (Conn. App. Ct. 2014). In resolving what constitutes "publication," the court averred, "[r]egardless of the precise definition of publication, we believe that access is a necessary prerequisite to the communication or disclosure of personal information." Based on *Recall*'s interpretation of the "publication" requirement, there must be proof of a third party's after-the-fact access to the recorded conversations for the offense to be satisfied.

Another coverage case arising out of a data breach found the insurer had no duty to defend because the "publication" was perpetrated by the hackers, not the insured. *See Zurich Am. Ins. Co. v. Sony Corp. of Am.*, Index Number 651982/2011 (N.Y. Sup. Ct. Feb. 21, 2014). This case can be useful for insurers because it demands that there be an affirmative act on behalf of the insured in order for there to be coverage. This further supports the interpretation of "publication" as requiring an affirmative disclosure of information to a third party.

By contrast, a Virginia federal district court held in a non-data breach case that there was a "publication" of material, despite that the theory alleged against the insured was one of passive negligence. *Travelers Indem. Co. of Am. v. Portal Healthcare Solutions*, LLC, No. 1:13-cv-917 (GBL), 2014 U.S. Dist. LEXIS 110987 (E.D. Va. Aug. 7, 2014). Specifically, the district court found that the insured's alleged failure to safeguard confidential medical records that were posted on the Internet constituted a "publication," despite there being no evidence or allegation that anyone actually viewed or accessed them. The district court reasoned that "the issue cannot be whether Portal intentionally exposed the records to public viewing since the definition of 'publication' does not hinge on the would-be publisher's intent. Rather, it hinges on whether the information was placed before the public." The court thus rejected the insurer's intent-based construction of the Privacy Offense. The district court also rejected Travelers' argument that third-party access to the confidential information was necessary for there to be a "publication." The district court analogized the situation to the publication of a book and explained that a book is published as soon as it is bound and placed on the shelves of a store. Thus, the district court concluded that "the medical records were published the moment they became accessible to the public via online search." Notably, the district court rejected the reasoning used in the FACTA cases and by the *Recall* court.

IV. Which Exclusions May Limit Or Bar Coverage?

If an insurer does not succeed on its "publication" defense, several exclusions found in standard ISO CGL policies may bar coverage entirely. This section will review the exclusions germane to unauthorized recording claims.

Criminal Acts Exclusion/Penal Statute Exclusion

As its name indicates, the criminal acts exclusion bars coverage for acts "[a]rising out of a criminal act committed by or at the direction of any insured. . . ." In *Bowyer*, *supra*, the Supreme Court of Appeals of West Virginia considered whether the exclusion absolved Westfield of liability since a violation of the WESA, which was the basis for the claimants against the insurer, is a felony. Yet, the Supreme Court insisted that the exclusion applies only where the insured is shown to have maintained "criminal intent." Since the hotel owner was allegedly told that the surveillance system was completely legal, there was no criminal intent.[7] Thus, the exclusion was deemed inapplicable.

Violation Of Law Exclusion

A relatively new exclusion is the Violation of Law exclusion. It bars coverage for any action or omission that that violates or allegedly violates "[a]ny federal, state or local statute, ordinance or regulation . . . that addresses, prohibits or limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating, or distribution of material or information."

The Violation of Law exclusion has already had an important impact on decisions in the surveillance context. In *Encore*, this exclusion was decisive in the court's decision that two insurers did not need to provide coverage, while another insurer, whose umbrella policies did not contain a violation of law exclusion, was required to defend the insured. *See* 2013 U.S. Dist. LEXIS 93513, at *14–15. Similarly, in *Urban Outfitters*, the Violation of Law exclusion relieved the insurer of its duty to defend its insured against alleged violations of the Song-Beverly Act since the ZIP code allegations arose out of a violation that prohibited the collecting or *recording* of information. 21 F. Supp. 3d

at 440. Clearly, this exclusion is a powerful tool for insurers to combat liability based on class actions brought under anti-recording statutes. This exclusion, given its broad scope, should also apply to actions for negligence or other common law torts based on the same conduct giving rise to the violations of the ECPA or state anti-recording statutes. *See G.M. Sign, infra.*

Violation Of Statutes Exclusion

Although the language of the Violation of Statutes exclusion is not as sweeping as the Violation of Law exclusion, it still should preclude coverage for unauthorized recording claims. The Violation of Statutes exclusion bars coverage for " 'personal and advertising injury' arising directly or indirectly out of any action or omission that violates or is alleged to violate . . . [a]ny statute, ordinance or regulation . . . that prohibits or limits the sending, transmitting, communication, or distribution of material or information."

Due to the language of this exclusion, policyholders argue that courts should not exclude coverage in surveillance cases because the term "recording" is not included. However, the following authority supports that the lack of the term "recording" is not outcome-determinative. First, in discussing an underlying FACTA action, one district court found that electronically printed receipts fell directly within the "communication or distribution" language of the exclusion. *Creative Hospitality Ventures, Inc. v. U.S. Liab. Ins. Co.*, 655 F. Supp. 2d 1316 (S.D. Fla. 2009). Also, in a ZIP code case, the Violation of Statutes exclusions[8] barred coverage for claims based upon alleged violations of the Song-Beverly Act. *Big 5 Sporting Goods Corp. v. Zurich Am. Ins. Co.*, 957 F. Supp. 2d 1135, 1156 (C.D. Cal. 2013). Because coverage for electronic surveillance actions is tied to a "publication," it stands to reason that the Violation of Statutes' language regarding statutes that prohibit the communication or distribution of material or information should also apply to alleged violations of anti-recording laws. Further, multiple courts, including the only court authoring a published opinion, have found that the Violation of Statutes exclusion applies to preclude coverage for tort causes of action ancillary to the violation of the expressly excluded statute, thereby precluding a duty to defend. *See, e.g., G.M. Sign, Inc. v. State Farm Fire & Cas. Co.*, 2014 IL App. (2d) 130593, 18 N.E.3d 70.

Access Or Disclosure Of Confidential Or Personal Information Exclusion

ISO has recently come out with a new exclusion in response to the wave of data breach suits, entitled "Exclusion – Access or Disclosure of Confidential or Personal Information and Data Related Liability – With Limited Bodily Injury Exception" (CG 21 06 05 14). The exclusion applies to:

> "Personal and advertising injury" arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information.
>
> This exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of any access to or disclosure of any person's or organization's confidential or personal information.

There is a viable argument that the exclusion applies to unauthorized recording claims because those claims allegedly involve the disclosure, *i.e.*, "publication," of the claimants' confidential or personal information. Specifically, that may include the claimant's credit card, financial information, or other "nonpublic information" revealed to the insured during the call recorded without the insured's consent. Unauthorized recording claims could also fall under the catch-all language, "any other type of nonpublic information." Because this exclusion is too new to have been construed by a court, it still remains to be seen how it will be applied to non-data breach claims.

Employment-Related Practices Exclusion

Another exclusion that may limit coverage for unauthorized recording claims is the employment-related practices exclusion. Generally, this exclusion applies to acts "arising out of any . . . employment-related practices, policies, acts or omissions such as coercion, . . . harassment, humiliation, or discrimination directed towards that person." This exclusion's relevance, however, should be restricted to surveillance cases when a claim is tendered by an employee, not a customer.

That is significant for cases like *Bowyer*, which involved an employee who sued his employer for a violation of WESA. Westfield asserted that the employment-related practices exclusion barred coverage. Nevertheless, the Supreme Court quickly rejected the argument because it opined that there was nothing in the record "to suggest that that appellant Hi-Lad, Inc. made it a practice, or had a policy, or engaged in, acts of humiliation."

The plaintiff in *NWM-Oklahoma*, among several other claims, also claimed that she was wrongfully terminated from her employment. The district court's decision could not have been easier because National Fire's employment-related practices exclusion expressly stated that the insurance did not apply to "[t]ermination of that person's employment[.]" Therefore, the court concluded that the policy's coverage excluded the wrongful termination claim.

In sum, the employment-related practices exclusion could be a powerful exclusion for insurers with regard to the category of unauthorized recording claims brought by employees.

V. Are Statutory Awards Insurable Under CGL Policies?

Even if an unauthorized recording claim triggers an insurer's duty to defend, another defense may greatly limit the insurer's exposure. CGL insurance policies generally state that the insurer will "pay those sums that you or any insured becomes legally obligated to pay as damages because of 'personal and advertising injury'. . . ." The statutory awards resulting from the anti-surveillance statutes, which are the big draws for class action attorneys, beg the question of whether the awards constitute "damages." Likewise, CGL policies may contain an exclusion for punitive damages. Applicable public policy may also deem punitive damages uninsurable. Ultimately, whether statutory damage awards are covered under CGL policies may be determinative of whether the insurer has a duty to indemnify its insured against a judgment or settlement arising out of the underlying class action lawsuit.

No court has decided whether statutory damage awards under the ECPA or similar state statutes are covered under a CGL policy. However, courts in other contexts have directly addressed the issue. For instance, the district court in *Big 5* concluded that civil penalties under the Song-Beverly Act did not constitute "damages." Similarly, the San Diego County Superior Court held that CGL policies did not cover statutory penalties under the Song-Beverly Act. *Arch Ins. Co. v. Michaels Stores, Inc.*, No. 37-2011-00097053-CU-IC-CTL. Moreover, a Pennsylvania district court found statutory damages under FACTA are not compensatory in nature and instead are inherently punitive. *See Whole Enchilada, Inc. v. Travelers Prop. Cas. Co. of Am.*, 581 F. Supp. 2d 677 (W.D. Pa. 2008).

By contrast, numerous courts have concluded that statutory awards under the TCPA are not penal or punitive in nature; instead, they are remedial, a liquidated sum designed to compensate the victims, and an incentive for claimants to bring suit. See, e.g., *Columbia Cas. Co. v. Hiar Holding, L.L.C.*, 411 S.W.3d 258 (Mo. 2013); *Std. Mut. Ins. Co. v. Lay*, 2013 IL 114617, 989 N.E.2d 591; *Motorists Mut. Ins. Co. v. Dandy-Jim, Inc.*, 182 Ohio App. 3d 311, 912 N.E.2d 659 (8th Dist. 2009); *Penzer v. Transp. Ins. Co.*, 545 F.3d 1303 (11th Cir. 2008); *Terra Nova Ins. Co. v. Fray-Witzer*, 449 Mass. 406, 869 N.E.2d 565 (2007).

The issue of whether statutory penalties constitute "damages" is incredibly important in the surveillance context since some of the statutes, like California's, allow statutory damages which can generate tremendous awards. If courts in California and elsewhere import the reasoning from *Big 5* and *Michaels Stores* to the surveillance context, it would provide a strong justification that those statutory damages are not insurable under CGL policies, thereby disincentivizing plaintiff class action attorneys from bringing these actions geared toward generating significant attorney fee awards.

Even if the statutory damage awards are insurable, a per claim or per claimant deductible may greatly limit an insurer's duty to indemnify its insured against such awards. As discussed above, most statutory schemes award claimants, at most, between $1,000-$10,000. Accordingly, a $10,000 per claim or claimant deductible may completely preclude any duty to indemnify the insured against the judgment or settlement. *See Alea London v. Am. Home Servs.*, 638 F.3d 768 (11th Cir. 2011) (upholds $500 per claimant deductible); *W. Heritage Ins. v. Love*, 24 F. Supp. 3d 866 (W.D. Mo. 2014) (deductible applies separately to each class member's claim based on each fax received).

VI. Conclusion

The fear of class action litigation from consumers under surveillance statutes is a very real threat to many insureds. In past year alone, more than 100 class action cases have been filed in California alleging violations of the anti-recording statute. *See e.g.*, Milligan & Salinas, *supra.* Similar statutes exist in myriad other states, too. And these claims show no signs of abating. In particular, claims against insureds who record their employees in an unauthorized manner will continue to face liability under the anti-recording statutes. Further, the surreptitious recording and dissemination of conversations (à la Donald Sterling) has never been easier with the proliferation of smart phones. Thus, a continuous flow of these claims is assured.

To date, the coverage jurisprudence for surveillance cases where the Privacy Offense's "publication" requirement is at issue has been mixed. There is a split among courts as to whether there must be a dissemination of the claimants' information to a third party. Future decisions will likely continue to divide on the "publication" issue. Yet, insurers can take solace in knowing that courts' interpretation of the "publication" requirement in similar situations provides them with some insight into how the courts will decide this vital issue in the surveillance context.

Moreover, these claims for coverage may not be a fixture in the future, as in 2013, ISO created an Amendment of Personal and Advertising Injury Definition Endorsement (No. CG 24 13 04 14), which eliminates the Privacy Offense. This reflects an intent to narrow personal and advertising injury coverage, as insurers have grown wary of providing coverage for consumer privacy claims. This endorsement has not become standard yet, but the momentum in favor of selling privacy coverage in specialty risk policies is gaining steam.

Additionally, the Violation of Statutes, Violation of Law, and Access or Disclosure of Confidential or Personal Information exclusions should play an important role in determining whether an insurer ultimately has a duty to defend and indemnify its insured. Therefore, insurers have the tools, even if the "publication" requirement is satisfied, to limit their liability in connection with high exposure surveillance claims.

Yet, it is imperative that insurers be proactive about using their tools. That means taking steps to protect their right to contest liability in their preferred forum, should that be the federal courts. According to the Anti-Aggregation Rule, separate and distinct claims by two or more plaintiffs cannot be aggregated to satisfy the $75,000 amount in controversy requirement. *See Travelers Prop. Cas. v. Good*, 689 F.3d 714 (7th Cir. 2012). Accordingly, if the insurer disclaims coverage, and the insured settles the class action lawsuit for an amount that pays each claimant less than $75,000, insurers may be foreclosed from initiating a declaratory judgment action in federal court to adjudicate coverage for the class settlement. *See Siding & Insulation v. Acuity Mut. Ins. Co.*, 754 F.3d 367 (6th Cir. 2014); *CE Design Ltd. v. Am. Econ. Ins. Co.*, 755 F.3d 39 (1st Cir. 2014). That does not mean the insurers will be unable to adjudicate coverage in any court, only that any such action would need to be brought in state court. That is true even if the insured or class consents to litigation in federal court. The most prudent approach, therefore, should be to consult early on with coverage counsel to determine what the recommended course of action should be with regard to the particular claim.

Endnotes

1. Sterling also received a $2.5 million fine. Although, in an incredible turn of karmic injustice, Sterling sold the Clippers for an unfathomable $2 billion.

2. InterContinental Hotels Group PLC recently filed in the United States District Court for the Northern District of California a breach of contract and declaratory judgment action against its insurers arising out of their refusal to defend and indemnify against the class action lawsuit. The lawsuit is encaptioned, *Intercontinental Hotels Group Resources, Inc. et al. v. Zurich American Insurance Co.*, No. 3:14-cv-4779.

3. This article uses the terms "electronic surveillance claims" and "unauthorized recording claims" interchangeably. The authors do not intend any difference between the two.

4. There generally is not much dispute over whether the underlying lawsuit alleges a violation of a person's "right of privacy." That is if the information being recorded or disseminated is a person's personal

identification information, such as a social security number or credit card number. *See Defender Sec. Co. v. First Mercury Ins. Co.*, No. 1:13-cv-00245-SEB-DKL, 2014 U.S. Dist. LEXIS 33318, at *10 fn.1 (S.D. Ind. Mar. 14, 2014) (recognizing that the claimant disclosed personal information during the call). The mere act of the insured recording a call, without the customer's consent, should not satisfy this requirement if the customer does not reveal any private information. *See Aquino v. Bulletin Co.*, 190 Pa. Super. 528, 533-34, 154 A.2d 422 (1959) ("there is no invasion of a right of privacy in the description of the ordinary comings and goings of a person"); *McNutt v. N.M. State Trib. Co.*, 88 N.M. 162, 166, 538 P.2d 804 (N.M. App. 1975) ("The address of most persons appears in many public records: voting registration rolls, property assessment rolls, motor vehicle registration rolls, etc., all of which are open to public inspection. They also usually appear in such places as the telephone directory and city directory which are available to public inspection."); *Tobin v. Mich. Civil Serv. Comm'n*, 416 Mich. 661, 674, 331 N.W.2d 184 (1982) ("Names and addresses are not ordinarily personal, intimate, or embarrassing pieces of information. . . . The plaintiffs' claim that disclosure of their names and addresses would intrude upon their privacy must also fail because the plaintiffs have suggested absolutely nothing objectionable about the method by which the information was obtained or is proposed to be released."); *but cf. Encore Receivable*, 2013 U.S. Dist. LEXIS 93513, at *26 (rejecting the carriers' argument that eavesdropping is not an act of communication to the public, but rather an invasion of seclusion accomplished by a non-communicative act).

5. This opinion was subsequently vacated. 2014 U.S. Dist. LEXIS 146083 (S.D. Ohio May 19, 2014).

6. However, with regard to another of the underlying actions, the district court concluded that the "publication" requirement was satisfied because Urban Outfitters allegedly disseminated information to third party vendors and retailers for marketing purposes. Due to the broad dissemination of the customer ZIP code information, the district court stated that "the matter must be regarded as likely to become public knowledge."

7. The criminal act exclusion was also at issue in *Encore*. There, plaintiffs in both underlying actions alleged criminal violations of the California Penal Code which prohibited unauthorized recordings. While the court noted that the exclusion does not require the insured to be convicted of a crime, the district court nonetheless found the exclusion inapplicable because it was a disputed issue of fact in both underlying actions whether a criminal act was even committed.

8. Interestingly, one "Violation of Statutes Exclusion" closely resembled the "Violation of Law Exclusion" because of the inclusion of the term "recording." ■

MEALEY'S: EMERGING INSURANCE DISPUTES
edited by Jennifer Hans
The Report is produced twice monthly by

1600 John F. Kennedy Blvd., Suite 1655, Philadelphia, PA 19103, USA
Telephone: (215)564-1788 1-800-MEALEYS (1-800-632-5397)
Email: mealeyinfo@lexisnexis.com
Web site: http://www.lexisnexis.com/mealeys
ISSN 1087-139X