COUGHLIN DUFFY LLP

ATTORNEYS AT LAW

Developments in Cyber Liability Claims: How Strong is Your Coverage Firewall?

Kevin T. Coughlin, Esq.
Sally A. Clements, 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, 28TH FLOOR
NEW YORK, NEW YORK 10005
PHONE: (212) 483-0105
FACSIMILE: (212) 480-3899

WWW.COUGHLINDUFFY.COM

TABLE OF CONTENTS

I. INTRODUCTION

Over the past decade, the world has become integrated and interconnected by the developments in technology and the ability to communicate and transact business over the internet. By necessity, we are dependent on the systems and infrastructure that supports this interaction, and as a result vulnerable to loss occasioned by disruption through hacking or service outages.

Recent years have seen a rapid expansion of the world's use of social networking sites, with sites such as Facebook, Twitter and LinkedIn replacing email and texts as the new communication method for both individuals and companies. While at the same time individuals are sharing more information with the public, they are also challenging on a regular basis companies use of their personal identifying information and the tracking of their locations and computer usage.

This greater use of social networking sites and, in fact, the significant increase in recent years of the use of electronic communications for consumers' online banking and purchases and companies' financial transactions and business procurement has exposed an increasing number of users to risk of loss of their personal identifying information. Companies are faced daily with a risk of cyber attacks that may be politically, personally or commercially motivated with a breach of their customers' as the end result.

The cost to companies to recover from a cyber attack and defend against resulting class action suits can be staggering. By one report, these costs have been estimated at between US $100,000 to $1 million per attack with the largest breaches costing in excess

of $100 million per attack.[1] A second report notes that data breach costs are climbing higher with estimated costs of $214 per compromised record and an average of $7.2 million per data breach event.[2] Regardless of the actual number, these costs can be significant and may include defense costs for class actions as well as ultimate liability that could include reissuance of credit cards, one or more years of credit report monitoring, premiums for additional insurance protection for the individual whose data was breached, reimbursement in goods or money for lost services. A data breach and the accompanying costs can be devastating to the impacted business.

With the increase in the number and severity of cyber liability claims, the number of cyber-related insurance claims is increasing, by one report as much as 56% over the past year.[3] We are seeing a slow development of the U.S. case law in this area as insureds look to specialty cyber liability policies as well as traditional first and third party liability policies to cover these claims. Below we address in greater detail the new cyber liability claims of the past year and the recent case law in this evolving claim type.

II. Current Trends in Cyber Claims

A. Data Breach Claims

With the year only three quarters complete, 2011 is already being heralded as the "Year of the Breach" referring to the number and severity of the electronic data breaches that occurred since January 2011.[4] Some of the most prominent so far in 2011 are:

- February – Nasdaq confidential data sharing service compromised

---

[1] Willis Group Holdings, "Willis: Leisure Industry Proves Irresistible Target for Cyber Pirates," ("Willis Report") 2 Aug. 2011, http://online.barrons.com/article/PR-CO-20110802-908350.html (last accessed 29 Sept. 2011).
[2] Larry Ponemon, "Cost of a Data Breach Climbs Higher," www.indefenseofdata.com, 8 March 2011.
[3] Willis Report, supra, at p.1.
[4] Law360, "2011 – The Year of the Breach," www.law360.com/insurance/articles/262849, last accessed 10 August 2011.

- March - Security firm RSA reports data related to SecurID token technology stolen
- April – Epsilon mail system hacked that contained data on customers of 50 retailers including U.S. Bank JPMorgan Chase, Capital One, Citi and others; Sony PlayStation Network data breach affects nearly 77 million subscribers.
- June – Dropbox cloud service provider – programming bug leaves 25 million user accounts accessible with any password;[5] Sony Pictures Entertainment systems are hacked potentially exposing 37,500 customers' personal information.[6]

The large number of records involved in data breaches in 2011 reflect a potentially significant increase from those involved in documented breaches in 2010. For example, in the report, "2011 Data Breach Investigations Report (DBIR)," the Verizon RISK Team, a data breach investigative response team at Verizon, in conjunction with the United States Secret Service and the Dutch High Tech Crime Unit, document in 2010 a drop in the total number of records compromised by data breaches over the prior two years.[7] Their 2011 report of 2010 statistics notes that Verizon has seen "the all-time lowest amount of data loss occur[ ] in the same year as the all-time highest amount of

[5] *Id.*
[6] Nick Bilton, "New Questions as Sony is Hacked Again," The New York Times.com, June 8, 2011.
[7] Wade Baker et al., "2011 Data Breach Investigations Report," Verizon RISK team, 2011. The Verizon RISK Team, a division of Verizon, a a leading internet service provider in the U.S., is involved in the investigation, restoration of services and protection of evidence following a breach of customer data. The RISK Team uses customers' data to compile its yearly report concerning the scope and source of data breaches.

incidents investigated."[8] In apparent contrast to 2011, a larger number of data breaches occurred in 2010, but each breach affected a smaller number of a records.

Verizon outlines the following entities involved in data breaches in 2010:

92% stemmed from external agents (+22% from prior year)

17% implicated insiders (-31%)

<1% resulted from business partners (-10%)

9% involved multiple parties (-18%)[9]

The circumstances of the data breaches in 2010 were:

50% utilized some form of hacking (+10% from prior year)

49% incorporated malware (+11%)

29% involved physical attacks (+14%)

17% resulted from privilege misuse (-31%)

11% employed social tactics (-17%)

As suggested above, most data breach occurrences in 2010 stemmed from hacking or installed malware by entities or individuals outside the firm and there was actually a drop in data breaches that involved an employee of the company. This is in contrast to Verizon's prior prediction that the global financial crisis would spur additional insider-related data breaches. In 2010, Verizon reportedly witnessed "highly automated and prolific external attacks, low and slow attacks, intricate internal fraud rings, country-wide device tampering schemes, cunning social engineering plots, and much more."[10] The United State Secret Service, the federal law enforcement agency originally formed to combat U.S. currency counterfeiting now also combats worldwide financial and computer

[8] *Id.*
[9] *Id.*
[10] *Id.* at 2.

cybercrimes. By their report, "[i]n 2010, the Secret Service arrested more than 1,200 suspects for cybercrime violations. These investigations involved over $500 million in actual fraud loss and prevented approximately $7 billion in additional losses."[11]

As outlined above, there were a significant number of reported data breaches in 2010 and, if the reported headlines and preliminary figures are accurate, the number of breaches and number of affected data records may have substantially increased in 2011. The details of the major data breaches in 2011 to date are discussed below.

1. Sony PlayStation Network Data Breach

The data breach of 2011 is unquestionably the Sony PlayStation Data Breach.

Sony's Online Services were breached between April 17 and 19, 2011, exposing names, home addresses, email addresses, birthdates, usernames, passwords, logins, security questions, and credit card data belonging to approximately 75 million user accounts. Several months before the breach, security experts monitoring open internet forums apparently learned that Sony was using outdated versions of the Apache Web server software, which was "unpatched and had no firewall installed."[12] The issue was allegedly reported in an open forum monitored by Sony employees two to three months prior to the security breach.

Sony's network team detected unauthorized activity in the network of 130 servers on April 19, 2011. Specifically, machines were "rebooting when not scheduled to do so." On April 20, 2011, Sony engineers discovered evidence of "unauthorized intrusion" and that data had been removed from PSN servers. On that same date, Sony engineers shut down the PlayStation Network ("PSN"), taking 77 million PSN and Qriocity music

[11] *Id.* at 6.
[12] Testimony of Dr. Gene Stafford, Purdue University, before the House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade, May 4, 2011.

accounts offline. It thereafter retained certain computer security and forensic consulting firms to look into the intrusion.

On April 22, 2011, Sony acknowledged on its blog that its system had an "external intrusion", but made no mention of the loss of personal and financial data and issued no warning to its customers. On April 23, 2011, Sony forensic teams confirmed that intruders used "very sophisticated and aggressive techniques to obtain unauthorized access, hide their presence from system administrators, and escalate privileges inside the server." Sony retained another forensic team the following day with "highly specialized skills" to "determine the scope of the data theft." While Sony confirmed that user account details were compromised, it remained unsure as to whether any of the 12.3 million global credit cards stored on its servers were also compromised.

On April 26, 2011, Sony notified the public of the breach and resulting loss of personal and financial data. Over the next two days, Sony alerted various state regulatory agencies of the breach, and, on May 3, 2011, Sony's Chairman Kaz Hirai sent a letter detailing the breach to the United States Congressional Subcommittee on Commerce, Manufacturing, and Trade.

There are over 50 class action complaints against Sony Computer Entertainment America LLC, Sony Network Entertainment International LLC, Sony Online Entertainment LLC, and Sony Corporation of America (collectively "Sony") connected to the Sony data breach pending in state and federal courts in California, Connecticut, Florida, Massachusetts, Michigan, New Jersey, New York, Ohio, and Texas as well as three class actions in Canada.

The class actions seek damages and injunctive relief arising from the Sony data breach and include breach of warranty, negligent data security, violations of consumer rights of privacy, violation of California and United States statutes protecting electronic privacy and financial data, failure to protect those rights, and failure and ongoing refusal to timely inform consumers of unauthorized third party access to their credit card account and other nonpublic and private financial information.

Plaintiffs allege that Sony failed to maintain proper and adequate backups and/or redundant systems, failed to encrypt or adequately encrypt data and establish adequate firewalls to handle a server intrusion, and failed to provide prompt and adequate warnings of the security breach to users of its Products and Online Services. Sony misrepresented the quality and reliability of its Online Services and its ability to keep data secure, including without limitation its representations in its Privacy Policy. They further allege that Sony was aware of the scope of problems with its Online Services for several months prior to the security breach but failed to take substantial corrective action and took only minimal action in response to consumer complaints.

Plaintiffs allege damages as a result of the April 2011 security breach for their loss of personal and financial information, the risk of identity theft resulting from the data breach and the subsequent disruption of online services, including the PlayStation Network. Plaintiffs seek actual, compensatory, statutory, and punitive damages as well as restitution and disgorgement of all amounts obtained as a result of Sony's unlawful acts and omissions. Plaintiffs further seek an order enjoining Sony from continuing to falsely market and advertise its products and online services, concealing material information, and conducting business in accordance with the unlawful business practices

alleged. Plaintiffs also request that Sony be ordered to engage in a corrective notice campaign, to refund money paid for the defective products and online services, and to pay for credit monitoring for Plaintiffs and the Class.

Certain of the class action complaints against Sony allege loss of use of PlayStation 3 consoles, portable devices, and software. In one action, Plaintiff seeks replacement or recall defective game consoles. Other class action complaints allege loss of use of products designed and sold for play over the internet, specifically games such as Call of Duty Black Ops, WWE All-Stars, Madden, and Call of Duty Modern Warfare 2. These products, along with items for sale by Sony including avatar clothing, weapons, and other digital property for use in conjunction with Sony's Products and Online Services, have been impaired or rendered worthless by the disabling of Sony's Online Services, including PlayStation Network. Other lost products, services, and add-ons for purchase, include: (1) new and classic games, add-ons, and free demos; (2) movies and television shows for rent and for purchase; (3) exclusive content, like Qore; (4) multiplayer and free online gaming; (5) exclusive access to new games and PlayStation's virtual gaming platform; (6) trophies and awards for display on Facebook®; and (7) Anywhere on PSP.

Certain of the class action suits against Sony also include claims for loss of use of funds in the form of inaccessible "PSN Wallets." "PSN Wallets" are linked to users' credit or debit cards for the purchase add-ons, additional services, and other digital content. Certain of the Sony class action complaints claim a loss of third party pay services, including, but not limited to, Netflix and Hulu that provide video streaming

services over the PlayStation network. A handful of the class actions allege fear and apprehension of fraud and fear of future fraud and identity theft.

B. Privacy Policy Violations on Social Networking Sites

As of July 2011, Facebook reported over 740 million users[13] and other social networking sites such as LinkedIn reported 100 million members worldwide[14] and Twitter reported 1 million users.[15] These numbers are increasing daily and the potential and actual claims are increasing as a result. ACE Insurance identifies the following risks to companies in accessing and posting to social networking sites:

Employment Risks: Employers may face liability under the Fair Credit Reporting Act if social network sites are accessed in connection with an employment application without first obtaining the applicant's consent. Employers may also face liability for firings based on Facebook communications with other employees.[16]

Security Risks: Employees may download malware, spyware or viruses through social websites. Employers may be held liable for data breaches caused by this malware where the company's "social media-related security policies, procedures, and technical safeguards are inadequate."[17]

Intellectual Property and Media Risks: Infringement claims may be based on employees posting or reposting information belonging to others. Breach of contract claims may arise if the posted information is subject to a contract with a company's client. Employee discussions on social media sites may disclose third party trade secrets.

---

[13] http://www.facebook.com/press/info.php?timeline, last accessed 25 September 2011.
[14] http://blog.linkedin.com/2011/03/22/linkedin-100-million/, last accessed 25 September 2011.
[15] http://blog.twitter.com/, last accessed 25 September 2011.
[16] Toby Merrill, et al., "Social Media: The Business Benefits May be Enormous, But Can the Risk – Reputational, Legal, Operational – Be Mitigated?" ACE Group, April 2011, p. 5.
[17] *Id.* at p. 6.

Even positive statements by an employee on a social network site could result in liability to the company as improper advertisement.[18]

Defamation Claims: Employee or public posts on company social network sites may include defamatory statements about competitors, exposing the company to potential claims.[19]

Privacy Claims: Failure to protect the privacy of information provided by customers through social network sites or to comply with the Children's Online Privacy Protection Act may subject the company to claims.[20]

C. Recent Decision in Pleading Injury in Fact for Data Breach of Social Network Site Login Credentials

A Federal District Court in California recently addressed whether a plaintiff had adequately pleaded injury in fact, as required to confer jurisdiction on federal courts under Article III of the Constitution, where defendant failed to encrypt plaintiff's personally identifying information and at least one confirmed hacker accessed defendants systems and copied the email and social network login credentials of approximately 32 million registered users. *Claridge v. RockYou, Inc.*, 2011 U.S. Dist. LEXIS. 39145 (N.D. Calif. April 11, 2011). In *RockYou*, the defendant, a "publisher and developer of online services and applications for use with social networking sites such as Facebook, My Space, hi5 and Bebo." [*Id.* at *2] brought a motion to dismiss plaintiff's claims for failure to plead an injury-in-fact. RockYou subscribers provided the defendants with their login credentials for other social networking sites. Plaintiff asserted the novel theory that the putative class members pay for products and services they buy from

[18] *Id.*
[19] *Id.* at p. 7.
[20] *Id.*

defendant by providing their Personal Identifying Information ("PII") and that PII constitutes valuable property that lost value as a result of defendant's alleged role in contributing to the breach of plaintiffs' PII. *Id.* at **10-11. The Court held that, although it held doubts about plaintiff's ultimate ability to prove its novel damage theory, it would not dismiss the case at the outset on the grounds that as a matter of law plaintiff has failed plead injury in fact sufficient to support Article III standing. *Id.* at *12.

D. Location/Usage Tracking Suits

The last year has seen several high profile suits against phone manufacturers and application developers for surreptitious collection of location data from users' mobile devices. The most prominent of these have been such suits against Apple, Google, and Netflix.

1. Apple Usage Tracking

In late December 2010, two class action suits were simultaneously filed against Apple in the federal courts in California. In Freeman v. Apple, Inc. et al., Northern District of California, Case No. 5:10-cv-05881 (filed 23 December 2011) and Lalo v. Apple, Inc. et al., Northern District of California, Case No. 5:10-cv-05878 (filed 23 December 2010) plaintiffs allege privacy violations by Apple and certain independent application development companies. Both suits allege that Apple and the other defendants intercepted plaintiffs' personally identifying information by use of applications on the iPhone and iPad and transmitted that information to third-party advertisers without plaintiffs' consent and in violation of their legal rights.

Both the Freeman and Lalo suits seek class action certification, injunctive relief preventing Apple from further collecting and disseminating the personal information

and/or requiring more detailed disclosure and informed consent; and compensatory, treble and/or punitive damages. The Freeman Complaint alleges that "Plaintiffs and members of the proposed class were harmed in that their personal property – their computer – was hijacked by Defendants and turned into a device capable of spying on their every online move." Both the Freeman and Lola Complaints include Causes of Action for violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, violation of the California Consumer Legal Remedies Act, violation of California's Computer Crime Law, violation of the California Unfair Competition Law, and unjust enrichment/restitution. The Freeman Complaint also alleges common law trespass and conversion. The Lola Complaint also alleges violations of the Electronic Communications Privacy Act, 18 U.S.C. §2510 et seq. and violation of the California Unfair Competition Law.

2. Google Location Tracking

On June 9, 2011, a class action was filed against Google in the United States District Court for the Southern District of Florida. In Brown v. Google, Inc., Case No. 2:11-cv-11867-AC-MAR, the representative plaintiffs allege that Google's Android operating system installed on cell phones secretly recorded and stored comprehensive details of the owners' movements. The Android Operating System allegedly logs, records and stores users' locations based on latitude and longitude alongside a timestamp and the phone's unique device ID. Plaintiffs allege that even disabling the phone's GPS components did not affect the functionality of the Google tracking system. They allege that they were harmed by Google's accrual of personal location, movement and travel histories. They seek class certification, declaratory and injunctive relief to enjoin Google

from "continuing to omit its true intentions about tracking purchasers of its products" and enjoining Google from tracking its products users. Causes of action also include claims under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, violation of state unfair or deceptive acts laws, fraudulent and intentional misrepresentation and negligent misrepresentation. In addition to injunctive relief, they seek in excess of $50 million in damages and any available exemplary, treble or punitive damages.

The case is in its early stages and it is anticipated that Google will file a motion to dismiss.

3. Netflix Usage Tracking

Netflix operates an online subscription service that currently allows customers to rent DVDs and to stream online movies for instant viewing. This year, six separate class action suits were filed against Netflix in the Federal District Court for the Northern District of California alleging privacy violations for its practice of retaining, storing, and utilizing records containing its customers' credit card numbers, billing and contact information and sensitive video program viewing histories on its server computers. The cases were recently consolidated into a single action styled In re: Netflix Privacy Litigation, Northern District of California, Case No. 5:11-cv-00379 in which a Consolidated Class Action Complaint was filed on 12 September 2011.

In the Consolidated Complaint, plaintiffs allege that as a result of Netflix's storage of the above information, "Netflix maintains a veritable digital dossier on thousands, if not millions, of former subscribers. The records contain not only the former subscribers' credit car numbers, usernames and passwords, as well as billing/contact information, but also a highly detailed account of each individual's video programming

viewing history." Netflix's privacy policy advises that the information it gathers in the aggregate is provided to prospective partners, advertisers and other third parties. Plaintiffs allege that Netflix's practices violate the Video Privacy Protection Act of 1988 ("VPPA") Under the VPPA, video-programming providers are required to destroy personally identifiable information as soon as practicable but no later than one year from the date the information is no longer necessary for the purpose for which it was collected. Plaintiffs claim that Netflix's retention and use of customer personally identifiable information after clients have closed their accounts violates the VPPA. Plaintiffs seek a declaration that Netflix has violated the statutes outlined above, injunctive and equitable relief requiring Netflix to destroy former subscribers' personally identifiable information and viewing histories and for damages including $2,500 per violation under the VPPA.

E. Failure to Meet Committed Service Levels – Cloud Computing

A significant source of cyber liability claims arises from the insured's or the insured's outsider vendors' failure to provide system access or services according to agreed contracts. Over the past year, the most significant service outages occurred in April with the outage of Amazon's EC2 cloud service that left hundreds of companies without their systems for a four-day period and the Sony data breach that left Sony's Play Station network suspended for approximately one month.

The Amazon outage has been cited in support of the vulnerability of "cloud computing." Cloud computing involves offsite storage of programs and data that are accessed by the user over the internet.[21] Under a cloud computing model, the client does not maintain its own onsite servers. With this relinquishment of control over a

[21] Mark Koba, "Cloud Computing 101: Learning the Basics." CNBC.com, last accessed 25 September 2011.

company's systems to another company, it is argued that the company is subject to the increased risk of a service outage unless it takes steps to establish a backup service in the event of a service outage. As the use of cloud computing increases over the next few years, there will undoubtedly be an increase in resulting claims.

III. Insurance Coverage for Cyber Claims

A. Specialty Cyber-Risk Products

Over the past several years, insurers have developed new products to meet the insurance needs of their clients in response to the increased threat of cyber liability claims. Sold as either stand-alone products or additions to existing policies, specific coverage is now available for:

- Privacy and security liability
- Data Breach Crisis Management
- Business interruption or data loss
- Internet Media Liability[22]

Such policies are typically written on a claims-made and reported basis and provide worldwide coverage.[23] They are also typically written on a cost-inclusive basis, with limits quickly eroded by the significant cost of defending cyber liability claims. The following is an example of a policy endorsement providing cyber liability coverage.

> **Cyber liability**
>
> The **insurer** will indemnify the **insured** against compensatory damages or awards (including where applicable claimants' legal costs and expenses) for any **claim** arising from:
>
> a) the content of the **insured's** email, intranet, extranet or website

[22] Kevin P. Kalinich, "Cyber Insurance 2011 Update – Privacy and Security Exposure and Solutions," AON Risk Solutions, 2011, p. 5.
[23] *Id.*

(including its domain name, metatags and hyperlinks and the marketing and advertising of the **insured's professional practice** on the website), including alterations or additions made by a **hacker,** and due to:

i) the **insured's** infringements of any intellectual property rights, including any copyright, trademark, passing off or link to or framing of another page;

ii) any defamatory statement on the **insured's** website or in the **insured's** email, including and defamatory statement concerning a client or business competitor of the **insured**;

iii) the **insured's** breach of confidence or infringement of any right to privacy;

b) the **insured's** negligent transmission of a computer virus, worm, logic bomb or Trojan horse to anyone in the course of the **insured's professional practice** or to anyone who uses the **insured's** website in the course of their business;

c) the **insured's** unintentional unauthorized collection, misuse or failure to correctly protect any data concerning any customer or potential customer of the **insured** which is either confidential or subject to statutory restrictions on its use and which the **insured** obtained through the internet, extranet or website and hold electronically;

d) a third party's good faith reliance on a **hackers** fraudulent use of the **insured's** encrypted electronic signature, encrypted electronic certificate, email or website where there was a clear intention to cause the **insured** loss or obtain a personal gain for the **hacker**.[24]

Under the above endorsement, coverage is provided subject to certain exclusions for both data breaches and intellectual property violations. Such cyber liability policies may exclude coverage for claims related to unauthorized use of credit or debit cards by the insured or third parties as well as claims caused by interruption of service by an internet provider, telecommunications or utility provider. The policy may also affirmatively require as conditions precedent to coverage that the insured's computer systems be protected by firewalls, virus protection, backups and compliance with specific data protection laws.

[24] QBE Endorsement Preview "MSVCLE04032010-A1" (http://www.qbeeurope.com/professional-financial/cyber-liability.asp) last accessed 25 September 2011.

B. Resort to Property and CGL Policies – Coverage Issues

Insureds that do not purchase specific cyber liability policies or whose cyber claims will exhaust such specialty policies also have looked to their standard First Party Property Damage and Comprehensive General Liability ("CGL") policies to cover data breach and other cyber liability claims. Insureds have asserted claims under First Party Property Policies to repair and restore their internal servers and have looked to CGL policies to address both internal costs as well as third party claims arising from data breaches. A number of coverage issues have arisen as a result of these claims.

In an early decision addressing the applicability of standard policies to data breaches, the Federal District Court for the District of Arizona held in *American Guaranty & Liability Insurance v. Ingram Micro*, in the context of a first party property damage policy, that loss of use of a computer system as a result of a power outage constituted "property damage" covered under the policy.[25] AON Risk Solutions reports that in response to the *Ingram Micro* decision, many insurers modified the definition of tangible property in their CGL and Property insuring agreements to expressly exclude electronic data.[26] As a result, insureds, and more specifically their counsel, have turned to creative interpretations of the CGL policy's Coverage B to claim coverage for cyber liability claims.[27]

Typical CGL policies provide, in Coverage B, coverage for "sums that the insured becomes legally obligated to pay as damages because of 'personal and advertising injury' to which this insurance applies." The term "personal and advertising injury" in turn, may

---

[25] *American Guaranty & Liability Insurance v. Ingram Micro, Inc.*, 2000 U.S. Dist. LEXIS 7299, *8 (D.Az. Apr. 18, 2000). See also, *Eyeblaster, Inc. v. Fed. Ins. Co.* 613 F.3d 797 (8th Cir. 2010).

[26] *Id.*

[27] In recent years, CGL policies have included exclusions for first party cyber liability claims and any coverage analysis should include particular attention to available specific exclusions.

be defined as injury arising out of "[o]ral or written publication, in any manner, of material that violates a person's right of privacy." Relying on underlying allegations that data breaches include personal information of their customers, including, but not limited to, credit card data, insureds will argue that they are entitled to defense and indemnity under Coverage B on the basis that the class action complaints allege publication of material that violates customers' privacy rights.

The CGL policy does not typically define the term "publication" and where the policy refers to "publication, *in any manner*," the policyholder may urge a court to take a broad view of what will fall within the scope of Coverage B. There is little doubt that credit card numbers and other information of a personal nature is material that implicates a right of privacy. However, it is less certain whether insureds can show the required "publication" within the meaning of a CGL policy if the injury was occasioned by a theft, rather than an insured's affirmative publication of private information in the sense than the insured made private information known to others or disseminated private information to the public.

There are a finite number of published decisions across the U.S. that have addressed the issue of personal and advertising injury coverage arising out of the "publication" of material that violates a person's privacy rights. To date, none specifically address whether the violation of a person's privacy rights, due to the theft of personal information by a third-party, non-insured, implicates personal and advertising injury coverage under Coverage B. Insureds have and will argue that cases in other contexts, such as the sending of unsolicited faxes, misuse of credit card information, improper access to credit report information, and other purported privacy rights

violations, present analogous circumstances that support a claim for coverage under Coverage B. In each instance, given the absence of policy definitions setting forth the meaning of "publication" or "right of privacy," the courts purported to take a reasonable, common sense approach in order to resolve the question of policy interpretation. In some of the cases discussed below, the courts took a broad view of coverage, even where it would seem that there was no publication of private information within the meaning of the policy at issue. However, it is important to understand in reviewing these decisions that none of the decisions involves a case where the data was taken by a third party without a single affirmative overt act by the policyholder to disseminate the information. This distinction may be pivotal as U.S. courts begin to address the coverage issues relating to cyber attacks.

In recent years, a number of coverage cases throughout the United States have addressed whether a party's unsolicited sending of "blast faxes," in violation of the federal Telephone Consumer Protection Act ("TCPA"), 47 U.S.C. § 227, implicates personal and advertising injury coverage under Coverage B. In *Valley Forge Ins. Co. v. Swiderski Electronics*, the insured was sued in a civil action alleging TCPA violations after it sent the underlying plaintiff and numerous other individuals a fax advertisement with information on the sale, rental and service of various types of electronic equipment.[28] The insured's CGL policy defined personal and advertising injury to include "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[29] The Illinois Supreme Court's ruling in favor of coverage rested upon its broad interpretation of the terms "publication" and "right of privacy."[30]

[28] *Valley Forge Ins. Co. v. Swiderski Electronics, Inc.*, 223 *Ill.2d* 352, 355 (2006)
[29] *Id.* at 356 (emphasis added).

First, the Court determined that the complaints alleged "conduct by [the insured] that amounted to 'publication' in the ordinary sense of the word" because, by faxing its advertisements, "[the insured] published [them] in the general sense of communicating information to the public and in the sense of distributing copies of the advertisements to the public."[31] In construing the meaning of "publication," the Court looked to the Webster's Dictionary and Black's Law Dictionary definitions of the word. Id. at 366-67. Webster's defined publication as "communication (as of news or information) to the public" and, alternatively, as "the act or process of issuing copies . . . for general distribution to the public."[32] Meanwhile, Black's defined publication as, "[g]enerally, the act of declaring or announcing to the public" and, alternatively, as "[t]he offering or distribution of copies of a work to the public."[33]

In addition, the *Swiderski* Court also concluded that the "right of privacy" connotes both an interest in the secrecy of personal information as well as an interest in seclusion.[34] It based this conclusion on the dictionary definitions of "right of privacy," which included, among other things, "invasion of privacy by disclosure of private facts" and "the quality or state of being apart from the company or observation of others: seclusion."[35] After reviewing the various definitions of right of privacy, the Court held that "[u]nsolicited fax advertisements, the subject of the TCPA fax-ad claim, fall within th[e] category" of "material that violates a person's seclusion."[36]

---

[30] *Id.* at 367-69.
[31] *Id.* at 367.
[32] *Id.* at 366 (*citing* Webster's Third New International Dictionary 1836 (2002)).
[33] *Id.* at 367 (*citing* Black's Law Dictionary 1264 (8th ed. 2004)).
[34] *Id.* at 368.
[35] *Id.* at 367-68 (*citing* Black's Law Dictionary 843, 1350 (8th ed. 2004); Webster's Third New International Dictionary 1804 (2002)).
[36] *Id.* at 368.

Accordingly, the *Swiderski* Court found that the claim potentially fell within the CGL policy's advertising injury provision.[37] As alleged in the Complaint, the insured "engaged in the 'written . . . publication' of the advertisements" and the material published "qualifies as 'material that violates a person's right of privacy,' because, according to the complaint, the advertisements were sent without first obtaining the recipients' permission, and therefore violated their privacy interest in seclusion."[38] A number of other courts addressing coverage for TCPA fax claims have reached similarly-grounded conclusions in favor of coverage.[39]

Other courts, including California courts, have not been so expansive in extending personal and advertising injury coverage to TCPA fax claims. The CGL policy at issue in *ACS Systems, Inc. v. St. Paul Fire & Marine Ins. Co.* defined "advertising injury offense" to mean, in part, "[m]aking known to any person or organization written or spoken material that violates an individual's right of privacy."[40] After distinguishing the two meanings to the "right of privacy" -- the right to "secrecy" and the right to "seclusion" -- the *ACS* Court determined that the TCPA violations at issue in the underlying litigation implicated the violation of "seclusion" privacy.[41] Next, the Court looked to California's "last antecedent rule" to construe the meaning of "material that

---

[37] *Id.* at 368-69.
[38] *Id.*
[39] *See, e.g., Park Univ. Enterprises, Inc. v. American Cas. Co. of Reading, PA*, 442 F.3d 1239 (10th Cir. 2006); *Hooters of Augusta, Inc. v. American Global Ins. Co.*, 157 Fed Appx. 201 (11th Cir. 2005); *TIG Ins. Co. v. Dallas Basketball, Ltd.*, 129 S.W.3d 232 (Tex. App. 2004); *Motorists Mut. Ins. Co. v. Dandy-Jim, Inc.*, 182 OhioApp.3d 311 (2009); *Penzer v. Transportation Ins. Co.*, 29 So.3d 1000 (Fla. 2010); *Terra Nova Ins. Co. v. Fray-Witzer*, 449 Mass. 406 (2007); *Nautilus Ins. Co. v. Easy Drop Off, LLC*, 2007 U.S. Dist. LEXIS 42380 (N.D. Ill. 2007); *American Home Assurance Co. v. McLeod USA, Inc.*, 475 F.Supp.2d 766 (N.D. Ill. 2007).
[40] *ACS Systems, Inc. v. St. Paul Fire & Marine Ins. Co.*, 147 Cal.App.4th 137, 142 (2d Dist. 2007)
[41] *Id.* at 149.

violates an individual's right of privacy."[42] That rule provides that "qualifying words, phrases and clauses are to be applied to the words, phrases and clauses immediately preceding and are not to be construed as extending to or including others more remote."[43] According to the Court,

> Considered grammatically, the word "that" in "[m]aking known to any person or organization written or spoken material that violates an individual's right of privacy" can reasonably be interpreted only to refer to "material." We find that "material" is not only the last antecedent of "that" but is also its only antecedent. "That" does not refer to "making known." Thus this particular advertising offense only refers to "material that violates an individual's right of privacy," and does not refer to a "making known that violates an individual's right of privacy."[44]

Therefore, the *ACS* Court concluded that it is the content of written or spoken material, when, in this case, "made known" to a person or organization, that violates a person's right of privacy.[45] In other words, an advertising injury offence under the policy at issue in *St. Paul* "provides coverage only if the harmful content violates the secrecy right of privacy, and does not provide coverage for a violation of the seclusion right of privacy."[46] Because the faxes did not contain private information about the recipient and because private information was not communicated to third-parties, the Court held that there was no covered offense under the policy.[47] The California appellate court in *State Farm Gen. Ins. Co. v. J.T.'s Frames, Inc.* reached the same conclusion, and applied the "last

[42] *Id.* at 150.
[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id.* at 152.
[47] *Id.* at 150, 152.

antecedent rule," where the policy at issue defined advertising injury to include "oral or written publication of material that violates a person's right of privacy".[48]

Similarly, in denying coverage, other courts, including courts applying the law of New York's neighboring jurisdictions, New Jersey and Pennsylvania, have, in the TCPA fax context, focused on the content of the faxes, and whether any private material was published or "made known," rather than the privacy right of seclusion that was allegedly violated when the fax was sent to the recipient.[49] In *St. Paul Fire & Marine Ins. Co. v. Brother Int'l. Corp.*, the Third Circuit Court of Appeals noted, "[a] policy's 'failure to define a term should not send the Court scurrying to a dictionary hunting for ambiguity' if that term's meaning is unambiguous when read in context."[50]

In recent years, courts have also begun to address whether claims involving violations of the Fair and Accurate Transaction Act ("FACTA"), 15 U.S.C. § 1681c(g), which requires merchants to truncate customers' credit card numbers on receipts, potentially implicate personal and advertising injury coverage under Coverage B. Under FACTA, "no person that accepts credit cards or debit cards . . . shall print more than the last 5 digits of the card number" on the receipt.[51] In *Creative Hospitality Ventures, Inc. v.*

---

[48] *State Farm Gen. Ins. Co. v. J.T.'s Frames, Inc.*, 181 Cal.App.4th 429 (2d Dist 2010).

[49] *See, e.g., St. Paul Fire & Marine Ins. Co. v. Brother Int'l. Corp.*, 319 Fed. Appx. 121 (3d Cir. 200)(no duty to defend where advertising injury defined as "making known to any person or organization covered material that violates a person's right to privacy")(N.J. law); *Melrose Hotel Co. v. St. Paul Fire & Marine Ins. Co.*, 432 F.Supp.2d 488 (E.D. Pa. 2006)("making known to any person or organization covered material that violates a person's right to privacy" required that "the content contained in the covered material violate a person's right of privacy and must be made known to a third party")(PA. law); *Telecommunications Network Design and Paradise Distributing, Inc. v. The Brethren Mut. Ins. Co.*, 2010 Pa.Super. 155 (2010)("oral or written publication of material that violates a person's right of privacy").

[50] *Brother Int'l. Corp.*, 319 Fed. Appx. at 125 (*citing Melrose Hotel Co.*, 432 F.Supp.2d at 501-02). *See also, e.g., American States Ins. Co. v. Capital Associates of Jackson County, Inc.*, 392 F.3d 939 (11th Cir. 2004)(but noting that "invasion of privacy" language in policy "reasonably could be understood to cover improper disclosures of Social Security numbers, credit records, email addresses, and other details that could facilitate identity theft or spamming")[50]; *Auto-Owners Ins. Co. v. Websolv Computing, Inc.*, 580 F.3d 543 (7th Cir. 2009).

[51] 15 U.S.C. § 1681c(g).

United States Liability Ins. Co., two insured merchants filed declaratory judgment actions against their insurers seeking declarations that their CGL policies provided coverage for the class action complaints filed against them alleging FACTA violations.[52] Both policies at issue defined "personal and advertising injury" to include injury arising out of "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[53]

The *Creative Hospitality* case exemplifies the lengths to which certain courts may go to provide coverage where policy terms are undefined. Referring to the Webster's Dictionary and Black's Law Dictionary definitions of publication to require some form of public dissemination, the insurers argued that the insureds' production to the cardholder of a receipt containing the cardholder's own credit card number cannot constitute a "publication."[54] The Court did not accept the insurers' interpretation of publication, however, because it believed that "the policy language itself render[ed] [it] unjustifiedly narrow in that it covers "[o]ral or written publication, in any manner."[55] It stated that "[i]n considering the breadth of the phrase, 'publication, in any manner,' the Court finds it difficult to conceive of a more inclusive description of the categories of 'publication' to be covered in an insurance policy, particularly in light of Florida's insurance policy construction canon requiring courts to interpret coverage clauses 'in the broadest possible manner to [e]ffect the greatest extent of coverage'."[56] On that basis, the *Creative Hospitality* Court concluded that the insureds "participated in 'publication' of the

[52] *Creative Hospitality Ventures, Inc. v. United States Liability Ins. Co.*, 655 F.Supp.2d 1316 (S.D. Fla. 2009)
[53] *Id.* at 1327.
[54] *Creative Hospitality*, 655 F.Supp.2d at 1328.
[55] *Id.* at 1329 (emphasis in original).
[56] *Id.*

[underlying] plaintiffs' protected payment card information when they provided receipts to only the cardholders . . . even though the cardholders already were aware of the information printed on the receipts." Further, because the underlying complaints alleged that the plaintiffs had been "aggrieved by" and "suffered actual harm" as a result of the FACTA violations, the Court determined that the contentions of actual injury "fairly and potentially [brought] the [underlying] lawsuits within the coverage of the policies at issue to the extent that the policies cover 'personal and advertising injury' resulting from '[o]ral or written publication in any manner, of material that violates a person's right of privacy.'" [57]

On the other hand, the District Court for the Western District of Pennsylvania, in *Whole Enchilada, Inc. v. Travelers Property Cas. Co. of America*, found that a FACTA violation did not constitute "publication," under policy language that was not as expansive as that at issue in *Creative Hospitality*.[58] The relevant policy language in *Whole Enchilada* defined "personal injury" to include "[o]ral, written or electronic publication of material that appropriates a person's likeness, unreasonably places a person in a false light or gives unreasonable publicity to a person's private life."[59] According to the Court, this language, contained in an endorsement, "effectively change[d] the terms of the standard insuring agreement," which defined "personal and advertising injury" to include "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[60] Referring to the Webster's Dictionary and

[57] *Id.* at 1335 (emphasis in original).The *Creative Hospitality* Court ultimately found, based on the policies' particular exclusions for certain statutory violations, that one insurer had a coverage obligation to its insured but the other did not. *Id.* at 1341, 1342.
[58] *Whole Enchilada, Inc. v. Travelers Property Cas. Co. of America*, 581 F.Supp.2d 677 (W.D. Pa. 2008)
[59] *Id.* at 693.
[60] *Id.*

Black's Law Dictionary definitions of publication as involving an element of public dissemination, the *Whole Enchilada* Court found that:

> [T]he Complaint alleges only that the information printed on the receipt was handed to the class member at the point of sale and does not allege that the cardholder's information was in any way made generally known, announced publicly, disseminated to the public, or released for distribution . . . The Complaint only alleges that the information was provided to . . . the class members in violation of FACTA. It does not allege that Whole Enchilada is liable for "publication," as the printed receipts are not made generally known, publicly announced, nor disseminated to the public.[61]

Thus, there was no "publication" within the meaning of the policy.[62]

Other privacy cases have arisen in connection with insureds' alleged violations of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681. For example, in *Zurich American Insurance Company v. Fieldstone Mortgage Co.*, the insured was alleged in the underlying class action complaint to have improperly accessed individuals' credit information, in violation of FCRA's requirement that access be either consented to or for a permissible purpose, in order to mail those individuals "prescreened" mortgage finance offers.[63] The Zurich policy at issue defined "personal and advertising injury" to include "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[64] Because the policy did not define publication, the Court, in accordance with the relevant Maryland law on insurance policy construction, looked to the Webster's Dictionary definition of publication as the act of publishing, or "to produce or release for distribution," and determined that the "[t]he term 'publication' can easily be read here to

---

[61] *Id.* at 697 (emphasis added).
[62] *Id.* at 697-98.
[63] *Zurich American Insurance Company v. Fieldstone Mortgage Co.*, 2007 U.S. Dist LEXIS 81570 (D. Md. 2007)
[64] *Id.* at * 3-4.

encompass the printing and mailing of written solicitations."[65] Further, the Court held that publication need not be to a third-party.[66] According to the Court, while a phrase such as "'making known' implies discovery or a previous ignorance . . ., which would necessitate disclosure to an unaware third party[,] 'publication carries no such connotations'."[67] The *Fieldstone* Court further explained that "[n]or does the phrase "publication, in any manner, of material that violates a person's right to privacy" necessarily require that the published material [itself] contain information that is specifically protected by a right to privacy; that is, information that is secret."[68] Accordingly, the Court held that there was a coverage obligation where the insured improperly accessed the underlying plaintiffs' credit information under the FCRA (the privacy violation) and then sent business solicitation letters to the plaintiffs that did not contain private information (the publication).[69]

Coverage for a privacy right violation under Coverage B has also been found where the insured, a computer consultant, improperly accessed e-mail information from his customer's system.[70] The insured consultant's CGL policy defined "personal injury" to include "[o]ral or written publication of material that violates a person's rights of privacy."[71] The insured began working for the customer as a software programming consultant under a Service Agreement that provided, in part, that he would not, without

---

[65] *Id.* at *12-13.
[66] *Id.* at *14.
[67] *Id.* at *15.
[68] *Id.*
[69] *See also Pietras v. Sentry Ins. Co.*, 2007 U.S. Dist. LEXIS 16015 (N.D. Ill. 2007)(same reasoning and outcome, where FCRA privacy violation preceded solicitation for auto loan); *State Farm Fire & Cas. Co. v. National Research Center for College and University Admissions*, 445 F.3d 1100 (8th Cir. 2006)(gathering and disseminating personal information beyond disclosed terms of use was "personal injury" arising out of "oral or written publication of material that violates a person's right of privacy").
[70] *Tamm v. Hartford Fire Ins. Co.*, 16 Mass.L.Rep. 535, 2003 Mass. Super LEXIS 214 (Superior Ct. 2003).
[71] *Id.* at *3.

prior approval, disclose or use for his own benefit confidential information relating to the customer's business.[72] A dispute arose after the customer failed to pay a $38,000 invoice, claiming that the insured had already been compensated for his work.[73] The customer alleged in the underlying complaint against the insured that the insured had sent an e-mail to the customer's outside counsel stating that he "learned tonight that [the customer] is initiating [sic] litigation counsel via Palmer & Dodge [sic]."[74] It further alleged that the insured forwarded a copy of this e-mail to a Palmer & Dodge partner, and also to two other outside counsel for the customer, and that, "on information and belief, [the insured] ha[d] been accessing one or more private and confidential e-mail accounts of [the customer] and/or its executives."[75] "In addition to allegations of accessing and distributing information obtained in private email accounts, the [underlying] lawsuit also allege[d] that [the insured] 'threatened to contact a list of specific e-mail addresses for individuals at [one of the customer's investors] and for other employees at [the customer]."[76] In the declaratory judgment action filed by the insured, the insured alleged that, among other things, the underlying complaint states a claim for invasion of privacy triggering the duty to defend.[77]

The *Tamm* Court stated that:

> In order to trigger the duty to defend under the invasion of privacy language of the policy, an underlying complaint must allege two things: (1) an "oral or written publication" of (2) "materials that violate person's [sic] right of privacy." The [underlying] complaint alleges that [the insured] accessed the private e-mail accounts of [the

[72] *Id.* at *4.
[73] *Id.*
[74] *Id.* at *5.
[75] *Id.* at *5-6.
[76] *Id.* at *6.
[77] *Id.* at *10.

> customer] and its executives and sent these private communications and materials to several outside counsel for [the customer]. The allegations of sending theses private communications via e-mail to outside attorneys seemingly satisfies both prongs under the invasion of privacy clause of the policy.[78]

The Court added that even though the underlying complaint did not contain an explicit claim for invasion of privacy, its request that the insured be restrained from acquiring, accessing and distributing confidential information supported the determination that the complaint generally implicates a claim for invasion of privacy.[79] Accordingly, the *Tamm* Court granted the insured's motion for summary judgment and held that the insurer had a duty to defend "under the right of privacy provision of the policy."[80]

Likewise, coverage has been found where an insured allegedly disclosed private medical information, in violation of the Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.*[81] In *Lenscrafters, Inc. v. Liberty Mut. Fire Ins. Co.*, the underlying plaintiff filed a putative class action lawsuit against Lenscrafters, Inc. ("Lenscrafters"), EYEXAM of California, Inc. ("Eyexam") and other entities alleging that certain arrangements between the companies violated their patient confidentiality rights under the CMIA.[82] Specifically, it was alleged that Lenscrafters and Eyexam, which maintained places of business next to or near each other, violated patient confidentiality when medical information disclosed to optometrists employed by Eyexam in the course of the patient/doctor relationship was routinely and improperly disclosed to employees of Lenscrafters, and that Lenscrafters used this information for non-medical

---

[78] *Id.* at *11.
[79] *Id.* at *13.
[80] *Id.* at *13-15.
[81] *Lenscrafters, Inc. v. Liberty Mut. Fire Ins. Co.*, 2005 U.S. Dist. LEXIS 47185 (N.D. Cal. 2005).
[82] *Id.* at *4.

purposes, such as marketing and sales.[83] Lenscrafters instituted coverage litigation against two of its insurers, one of which, Liberty Mutual Fire Ins. Co. ("Liberty"), had issued CGL policies that defined "personal injury" to include "[o]ral or written publication of material that violates a person's right of privacy."[84] Liberty argued that its duty to defend was not triggered because the underlying complaint did not allege a "publication" that "violates a person's right of privacy."[85] Specifically, Liberty contended that the underlying complaint did not allege that Lenscrafters published any confidential medical information to third-parties but, rather, that Lenscrafters improperly led patients to believe that its employees were employees of Eyexam and that this misrepresentation created a false sense of confidentiality that caused the patients to disclose private information in the presence of Lenscrafters employees.[86]

The *Lenscrafters* Court began its analysis by noting that the term "publication" is not defined in the Liberty policies.[87] Accordingly, it referred to the Black's Law Dictionary definition of "publication" as, "[g]enerally, the act of declaring or announcing to the public."[88] It also observed that:

> [U]nder certain legal doctrines, "publication" does not require that the information-at-issue be widely disseminated. For example, for purposes of defamation law, "the definition of 'publication' is not restricted to widely disseminated materials such as magazines and newspapers." *Brown v. Kelly Broadcasting Co.*, 48 Cal.3d 711, 723 n.6, 257 Cal.Rptr. 708, 771 P.2d 406 91989). "It is not necessary that the defamatory material be communicated to a large or even a substantial group of persons. It is enough that it is communicated to a single individual other than the

[83] *Id.* at *5-6.
[84] *Id.* at *26.
[85] *Id.* at *27.
[86] *Id.* at *30-31.
[87] *Id.* at *30-31.
[88] *Id.* (*citing* Black's Law Dictionary 1242 (7th Ed. 1999)).

> one defamed."[89] *Id.*, citing, Rest.2d Torts, § 577, com. B, p.202.
>
> Reading the term in context, as the law requires, supports a finding that "publication of material that violates a person's right of privacy" does not require widespread disclosure. Although Liberty is correct that common law invasion of privacy by public disclosure of private facts requires that the actionable disclosure be widely published and not confined to a few persons or limited circumstances, nothing in the Liberty Policies limits "right of privacy" to common law right of privacy.
>
> * * *
>
> Given the many ways that publication of material can violate a person's right of privacy, and the fact that the clear language of the Liberty Policies does not limit "right to privacy" to just one type of right, it is not clear that the term should be limited as Liberty suggests.[90]

Under the foregoing principles, the *Lenscrafters* Court found that all of the alleged disclosures of private medical information were publications that violated a

---

[89] In fact, in the defamation context at least one California court post-*Lenscrafters* has found in favor of coverage under Coverage B "where the [defamatory] statements were not directly published by the defamers themselves" but instead communicated to the person who was defamed. *Diversified Communications Services, Inc. v. Landmark American Ins. Co.*, 2009 *U.S. Dist. Lexis* 27930 (C.D. Cal. 2009). In *Diversified*, three employees of the insured were alleged in an underlying litigation to have defamed the underlying plaintiff by directing racial epithets to him during the time he was employed by the insured. *Id.* at *1-2. Observing that the insured "correctly note[d] [that] no claim for slander lies if the defamatory statement was not 'published,' i.e., communicated to some third person who understands its defamatory meaning and application to the plaintiff," the Court also found that, under California law, '[p]ublication [of defamatory material] need not be to the public or a large group; communication to a single individual is sufficient." *Id.* at *18. The *Diversified* Court stated that, "at first blush, it appear[ed] as if the statements were never published," because the underlying complaint did not allege that anyone other than the defamers and the person defamed were in the shop at the time the statements were made. *Id.* The Court concluded, however, that "simply because the statements were not directly published by the defamers themselves does not necessarily mean that they were never published at all. In some cases, the originator of a statement may be liable for defamation when the person defamed republishes the statement, provided that the originator 'has reason to believe that the person defamed will be under a string compulsion to disclose the contents of the defamatory statement to a third person after he has read it or been informed of its contents." *Id.* Fortunately for the insurer in *Diversified*, the Court ultimately found that coverage was barred due to an Employment-Related Practices Exclusion in the policy at issue; otherwise, the Court would have held that the insurer had a duty to defend based on the policy's definition of "personal and advertising injury" as encompassing "[o]ral or written publication, in any manner, of material that slanders or libels a person or organization . . .". *Id.* at *10, *21-27.

[90] *Id.* at 31-34.

person's right of privacy.[91] It specifically noted that the underlying complaint alleged that defendants "caused" patients to disclose medical information to persons who were not under the direct supervision and control of optometrists and that defendants then "disclose[d] this confidential medical information to Lenscrafters for marketing and sales purposes."[92] According to the Court, the underlying complaint also alleged that defendants also "cause[d] and allow[ed]" medical records to be "accessed and reviewed" by employees who were not under the direct supervision and control of an optometrist and for non-medical reasons.[93] It therefore concluded that, "[a]ssuming that the term is ambiguous, based on the foregoing discussion, it is objectively reasonable that the term 'publication of material that violates a person's right of privacy' encompasses the types of disclosures alleged in the [underlying] action."[94] Thus, Liberty had a duty to defend Lenscrafters in the underlying litigation.[95]

Based on the *Lenscrafter* Court's reliance on cases addressing the meaning of "publication" in the defamation context, insureds may argue another basis for coverage under CGL policies. This is the concept of "negligent publication" under the law of defamation, namely, that defamatory information revealed by way of negligence is sufficient to constitute publication. On this issue, the Restatement (Second) of Torts § 577 states "[p]ublication of defamatory matter is its communication intentionally or by a negligent act to one other than the person defamed". Additionally, in *American Continental Ins. Co. v. Pooya*, the District of Columbia appellate court noted that "if liability were to rest on negligent publication, this would be covered under the disputed

[91] *Id.* at *36.
[92] *Id.* at *34.
[93] *Id.*
[94] *Id.* at *36.
[95] *Id.* at *45.

[professional liability] policy".[96] An insured may argue that it negligently caused or allowed private information to be accessed, for example, by not maintaining adequate "firewalls" or other protections, resulting in the publication of private information.

IV. CONCLUSIONS

As outlined above, 2011 has been an active year for cyber liability claims in the U.S. Significant data breach announcements by Sony and other companies have spurred claims across the country. Plaintiffs are bringing a number of suits challenging companies' tracking of their location and computer usage profiles while at the same time users are posting more of their personal information to social network sites than ever before.

The coverage issues surrounding coverage under both specialized policies and traditional CGL policies are still evolving through a small number of declaratory judgment actions in U.S. courts. It remains to be seen whether insureds will be able to fit these new and emerging claim types into the Coverage B of their CGL policy, originally designed for traditional personal injury claims. As discussed above, the outcome of such claims will be fact-sensitive and in many cases determined by the venue of the action and chosen law.

[96] *American Continental Ins. Co. v. Pooya*, 666 A.2d 1193 (D.C. App. 1995)