FirstLook

Issues and Developments in Insurance Law

LETTER FROM THE EDITOR

Pardon the quote from 1984's one-hit wonder Rockwell's hit, "I always feel like somebody's watching me" - but it's never been truer! Sure, the media spotlight is focused on NSA leaker Edward Snowden's efforts to avoid extradition and prosecution, but the real question lingers beyond headlines: "What government surveillance constitutes an unlawful violation of Fourth Amendment privacy rights?" In today's digital age, where electronic communication touches nearly every aspect of our life, what privacy rights do U.S. citizens have regarding their technological footprint - actual substance of emails, phone calls, and internet searches, among other things?

The increased use of technology in the workplace creates concern for both employers and employees in the privacy realm. Most employees have access to email, and internet access in the workplace has exploded. Obviously, technology can be lauded for the many ways that it's helped business, but simultaneously, it raises concerns that previously didn't exist. Employers have technological access to both work-related and personal information about their employees and want that information. Not surprisingly, employees are concerned about it.

There are legal frameworks which address privacy concerns. But when these concerns arise, employers may be open to invasion of privacy claims and accordingly, may seek coverage for those claims under their EPLI or CGL policies.

We hope this issue of First Look will help open your eyes, or if they are open, maybe open them a little wider to these claims which are no doubt on the rise. And where there are claims, we know insureds hope there's coverage!

Joanna I. Tabit, Esq.
Guest Editor
joanna.tabit@steptoe-johnson.com

To receive "First Look" electronically:
- Visit our website at www.steptoe-johnson.com
- Click on Know-How and complete the registration form

You will then receive "First Look" electronically and be given access to our electronic archive of useful insurance information.

INSIDE THIS EDITION:

"SOMEBODY'S WATCHING ME: THE CURRENT STATUS OF PRIVACY CLAIMS AND RELATED COVERAGE ISSUES"

IN THIS ISSUE

Private Eyes...

(Requests for Coverage for Privacy Claims Under CGL Policies)

By: Melanie Morgan Norris

The issue of privacy has risen to the forefront in this age of computer technology where nearly every task can be completed "online" and personal information is transmitted at warp speed through "cyberspace." The "right to privacy" has long existed in a variety of jurisdictions at common law, and over the years, some jurisdictions developed statutes and regulations protecting the right to privacy. Nonetheless, the increased awareness of privacy issues has generated a slew of new state and federal statutes aimed at further protecting privacy rights. The public's new awareness of privacy rights is beginning to generate more "privacy" claims. *See generally*, Matthew J. Schlesinger and Jason M. Silverman, *Insuring Privacy: Is Your Company Covered?*, Tort and Insurance Law Journal (2002).

In the insurance context, an increase in breach of privacy litigation translates into an increase in third-party claims against insureds, *inter alia*, an increase in requests for defense and indemnification. Privacy claims are generally grouped into four categories: (1) an allegation that the defendant has unreasonably intruded upon the "seclusion" of the claimant; (2) an allegation of an "appropriation" by the insured of the claimant's name or likeness; (3) an allegation of unreasonable publicity given by the insured to the claimant's private life, or; (4) an allegation that the insured has created or caused publicity that unreasonably places the claimant in a "false light" before the public. *See, e.g.*, Restatement of Torts 2d § 652A (2013). How the claim is presented depends upon the jurisdiction in which it is brought and whether privacy rights exist in that jurisdiction only at common law or whether they are also codified by statute.

Although the body of case law is not large, for some time, invasion of privacy type claims have potentially triggered coverage under the "personal and advertising injury" coverage grant of a Commercial General Liability (CGL) policy which traditionally has defined "personal and advertising injury," in part, as "oral or written publication, in any manner, of material that violates a person's right of privacy." *See, e.g.*, ISO form CG 00 01 10 01. Historically, the majority of cases addressing the availability of coverage for privacy claims under a CGL policy have arisen in the context of employment related cases. *See* Schlesinger and Silverman, *supra*. However, with the increase in legislation designed to protect privacy rights in this cyber age, new cases are cropping up that address coverage for privacy claims arising from violations of statutes designed to ensure privacy. *See, e.g.*, The Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2701-2711 (prohibiting unauthorized access to computers); The Telephone Consumer Protection Act ("TCPA"), 47 U.S.C. § 227 (prohibiting, in part, unsolicited advertisements by facsimile to telephone subscribers); Fair and Accurate Credit Transactions Act ("FACTA"), 15 U.S.C. § 16781 (protecting credit and debit card numbers).

As with any claim, whether there is coverage under a CGL policy for a privacy claim depends on the allegations giving rise to the claim in the first instance, the insuring language and any potentially applicable exclusions or endorsements. A threshold determination is whether the allegations in the complaint are sufficient to set forth a claim for the tort of invasion of privacy within the jurisdiction in which the claim is pending. If not, then coverage is never triggered under the "personal injury or advertising" coverage grant of the policy. *See, e.g.*, M. Jane Goode, *Law and Practice of Insurance Litigation*, §6:33 (June, 2013); *Cornhill Ins. PLC v. Valsamis, Inc.*, 106 F.3d 80 (5th Cir.), cert. denied, 522 U.S. 828 (1997). For example, in *Cornhill*, a former employee sued her employer for sexual harassment and other related claims. Faced with a subsequent suit to determine coverage, the *Cornhill* Court reasoned that under Texas law, the tort of invasion of privacy required proof that there was an intentional intrusion that was highly offensive, and that the tort was generally associated with physical invasion of a person's property or eavesdropping on another's conversation with wiretap. The Court concluded that the employee's allegations of offensive comments and inappropriate advances did not meet the tort elements necessary to establish an invasion of privacy offense, such that there was no "personal injury" under the policy.

Even if the allegations are sufficient to set forth a claim for the tort of invasion of privacy in the relevant jurisdiction, the insuring language must still be analyzed to determine whether coverage is triggered. In the employment context, there has been significant litigation over whether the claimed misconduct was "an offense arising out of [the insured's] business" as is required under the insuring agreement. *See, e.g.*, ISO form CG 00 01 10 01. For instance, in *St. Paul Guardian Ins. Co. v. Centrum GS, Ltd.*, 283 F.3d 709 (5th Cir. 2002), an employee brought suit against his former employer for, among other things, invasion of privacy. The employee contended that after he was terminated, the employer hired eight uniformed police officers to patrol the lobby of the building (owned and managed by the employer) and also put up "WANTED POSTERS" with the terminated employee's picture and personal identifying information, requesting that anyone who saw him in the building, contact security. *See id.* at 711. The carrier argued that the complained of privacy offense did not arise out of any "business activity." The Fifth Circuit disagreed. Noting that "business activity" was undefined in the policy, the court went on to find that the employer had posted the information concerning a perceived risk to its building and tenants "in a place where it could be viewed and appropriately used." The Court went on to hold that giving the term "business activity" its plain meaning, the employer's actions were "consistent with its business of owning and managing property." *See id.* at 174.

Another key issue that has received some attention from the courts in determining the viability of a third-party breach of privacy claim is whether a "publication" has occurred. Most CGL policies require a privacy violation to be based on an oral or written "publication" of material with the word "publication" undefined in the Policy. *See, e.g.*, *State Farm Fire and Cas. Co. v. National Research Center for College and Univ. Admissions*, 445 F.3d 1100 (8th Cir. 2006). In *National Research*, complaints were filed against a private research firm by the Federal Trade Commission and

state attorneys alleging that the firm had shared survey results of high school students with commercial entities instead of just educational entities as had been represented to the students. The court concluded that the research firm's gathering and disseminating of the information to commercial entities beyond disclosed terms was arguably an invasion of privacy by "oral or written publication" under Missouri law. *But see, Whole Enchilada, Inc. v. Travelers Prop. Cas. Co. of America*, 581 F. Supp. 2d 677 (W.D. Pa. 2008) (concluding that insured's alleged violation of FACTA by printing more than the last 5 digits of a credit card on receipts did not fall within the plain meaning of the term "publication" where the receipts were not made generally known, publicly announced, nor disseminated to the public).

Of course, all potentially applicable exclusions are scrutinized by the courts before determining whether coverage exists. For instance, most CGL policies contain "Criminal Acts" and "Knowing Violation Of Rights Of Another" exclusions, either of which may bar coverage for intentional invasions of privacy. *See, e.g.*, ISO form CG 00 01 10 01. Some courts have concluded, however, that an intentional acts exclusion renders coverage for invasion of privacy illusory, and have therefore interpreted the policy so as to provide coverage. *See, e.g.*, Couch on Insurance 3rd ed. § 127.3; *see also Linberry v. State Farm Fire & Cas. Co.*, 885 F. Supp. 1095, 1099 (M.D. Tenn. 1995) (concluding that all forms of invasion of privacy are intentional torts therefore rendering coverage for invasion of privacy illusory by virtue of the intentional acts exclusion); *Bailer v. Erie Ins. Exchange*, 344 Md. 515, 687 A.2d 1375, 1384 (1997) (holding policy language was ambiguous because it provided coverage for invasion of privacy under the "personal injury" coverage grant while also excluding coverage for personal injury expected or intended by the insured). Other jurisdictions, however, have reconciled the intentional acts exclusion by concluding that not all forms of invasion of privacy are intentional. *See, e.g., Fire Ins. Exch. v. Bentley*, 953 P.2d 1297, 1302 (Colo. Ct. App. 1998) (concluding that the policy provided coverage for some claims of invasion of privacy, but not those forms of invasion of privacy premised on intentional conduct); *Burns v. Middlesex Ins. Co.*, 558 A.2d 701 (Me. 1989) (holding that allegation of invasion of privacy does not automatically allege that the tortfeasor intended or foresaw bodily injury).

In more recent years, the insurance industry has reacted to the increasing state and federal statutory regulation of internet activity by including new exclusions within CGL policies that exclude coverage for "personal injury or advertising injury" arising out of statutory violations. *See* Harvey Nosowitz, Anderson & Kreiger LLP, *CGL Coverage for Invasion of Privacy: Recent Cases and Trends*, CGL Reporter (2011). A recent case addressing statutory violation exclusions in the context of a privacy claim is *Big 5 Sporting Goods Corp. v. Zuich American Ins. Co.*, -- F. Supp.2d -- , 2013 WL 3526039 (C.D Cal. July 10, 2013), In *Big 5*, the court was asked to determine the availability of coverage under two carriers' CGL policies issued to Big 5 which had been sued under a California state statute, the Song-Beverly Act, for recording and publishing customer zip codes during credit card transactions. *See id.* at * 1.

The first carrier's policy (Zurich's) contained a statutory violation exclusion, excluding coverage for personal injury arising directly or indirectly from the violation of "[a]ny federal, state or local statute, ordinance or regulation, other than the TCPA, CAN-SPAM Act of 2003 or FCRA, that relates to, prohibits or limits the accessing, collection, recording, printing, dissemination, disposal, sending, transmitting, communicating or distribution of material or information." The policy issued by the second carrier, Hartford, contained a similar exclusion. The Hartford policy also contained a second exclusion for personal injury arising "out of the violation of a person's right or privacy created by any state or federal act."

The *Big 5* Court concluded that each carriers' exclusion operated to bar coverage, reasoning that the legislative history of the Song-Beverly Act revealed that prior to its enactment, there was no common law invasion of privacy right that prevented businesses from requiring customers to provide zip codes in connection with credit card transactions. Because the narrow privacy right was statutorily created, and not based on common law, the court concluded that the claims were subject to the statutory exclusions. *See id.* at 15. The Court's analysis of whether the privacy claim is based in statute or common law could have significant implications depending upon whether the jurisdiction in which the claim is brought has common law privacy rights. As one commentator has noted, to the extent that a state has enacted legislation prohibiting publications in violation of privacy rights, such state statutes would appear to invoke the statutory violation exclusion in most policies. *See* Nosowitz, *supra*.

Finally, it should be noted that there are new insurance policies and endorsements popping up every day in the insurance industry designed to specifically afford coverage for privacy claims arising from a breach of personal information in cyberspace. These new coverages, such as the "cyber and technology services endorsement" or "information security and privacy liability insurance" are intended for optional purchase to supplement the traditional CGL Policy and provide specific protection for the unauthorized disclosure of data.

As technological advances (and mishaps) continue to increase, so will the attention that the public places on privacy concerns. The increased public awareness will necessarily translate into increased litigation and an increased breadth of case law interpreting the "personal and advertising injury" coverage grants and exclusions under CGL policies. Potential coverage for such claims must be carefully scrutinized when determining whether there is a duty to defend and a duty to indemnify. Not only must the insuring agreement and any potentially applicable exclusions be considered, but so must the specific elements of the alleged privacy tort in the relevant jurisdiction. Familiarity with the past "battlegrounds" for privacy coverage under traditional CGL policies, and familiarity with the new statutory exclusions will be key in making appropriate coverage determinations

Every Breath You Take...

(Coverage for Privacy Claims in EPLI Policies)

By: Tracey B. Eberling

With the explosion of employment practices claims and litigation, many employers sought protection by purchasing employment practices liability (EPLI) coverage and the insurance industry responded. Despite the increase in the number of EPLI policies written over the past few decades, the number of reported decisions concerning the scope of coverage is few. The lack of guidance by the courts, coupled with the fact that EPLI insurance essentially remains a specialty product with no standard form for coverage and exclusions, leaves both insurers and insureds uncertain about what claims may be covered and when a defense is owed. So, the answer to question of whether employees' privacy claims are covered is a resounding "it depends" – as it does in so many insurance coverage disputes - on the policy language and the nature of the claim asserted.

EPLI policies generally provide coverage for "wrongful employment practices" or "employment practices violations." These terms may be broadly or narrowly defined and generally include coverage for wrongful termination, discrimination and harassment. While some policies also offer coverage for retaliation, misrepresentation, libel, slander, and invasion of privacy, other policies specifically exclude such claims from coverage. Typically excluded are claims asserted under state and federal employment statutes such as workers compensation, ERISA, the Fair Labor Standards Act and the Occupational Health & Safety Act and for intentional acts. Risks covered by other policies are also generally excluded. EPLI policies may or may not coverage breaches of data security.

While "invasion of privacy" gets only a passing mention in EPLI policies, the scope of potential claims that could be asserted by employees or job applicants is seemingly unlimited. Consider the breadth of information that employers maintain about their employees and can readily access. Job applicants are often asked to permit the prospective employer to obtain a credit report or to run a criminal background check. Applicants and employees may also be subject to drug and alcohol testing, both pre-employment and as permitted by state law. Although now expressly prohibited by law in several states, employers sometimes request access to or information about the applicant's social media accounts, including passwords. Employers with self-insured or administered health plans necessarily maintain vast amounts of health information. Requests for accommodations under the ADA/ ADAAA or leave under the Family Medical Leave Act will also put employers in possession of otherwise private health information. Many employers monitor their employees' use of company-owned computers by tracking emails and internet usage, as well as telephone calls made on business lines and on company-provided cell or smart phones. While this may allow employers to assess productivity, such practices may net private information, including communications with employees' attorneys. Employers may also track the activities of employees by use of workplace surveillance cameras or by GPS units installed on company vehicles. These examples underscore the potential for inadvertent disclosure or wrongful use of private financial or health information or that may otherwise invade the privacy rights of employees.

The few identified cases involving EPLI policies thus far address whether employee wage claims are covered claims. In one such case, *Gauntlett v. Illinois Union Insurance Co.*, 2012 WL 4051218 (N.D. Cal. 2012), the employer creatively, but unsuccessfully, argued that its EPLI insurer should have provided a defense for an employee's claim for overtime compensation resulting from her alleged misclassification as an "exempt" employee. The insured asserted that its carrier should have requested additional information about the claim and had it done so, it would have identified facts supporting a potentially-covered claim for invasion of privacy.

The matter arose when the employee made a written demand for payment of unpaid overtime compensation that she believed she was entitled to receive. The following work day, she discovered that all of her stored email communications had been deleted. The company's IT professional confirmed that fact. The employee resigned when the employer declined to meet her deadline for payment, then filed suit, claiming violation of several California wage payment laws. The employee's complaint mentioned the deletion of her emails but notably omitted any reference to an expectation of privacy as to her computer and emails. The claim was reported and the employer's insurer denied the request for defense of the lawsuit on the bases that the damages sought did not fall within the policy's definition of a covered "loss" or were otherwise excluded under provisions related to compensation earned or due or that the claims were excluded "wage and hour" claims. The court granted the insurer's motion for summary judgment and denied the employer's subsequent motion for reconsideration of that ruling, declaring that the employer faced no potential liability for a covered claim under the complaint. The absence of any contention by the employee of expectation of privacy was critical to the decision. The employer's alternative argument that the misclassification of the employee as exempt from overtime compensation was a covered misrepresentation was also rejected.

Many EPLI carriers offer risk management services to their clients that can help them avoid claims, including those for invasion of privacy. Adoption of policies and practices by employers may be positively reflected in underwriting decisions such as reductions in premiums. For example, employee handbooks can be used to notify employees that their use of company-owned phones and computers may be monitored, thus limiting or perhaps removing employees' expectation of privacy. Encryption of health information and limiting access to that data can reduce the risks of misuse and inadvertent disclosure or access by outsiders.

Creative lawyering, by attorneys representing employees, employers and EPLI carriers, will define the future of employment-based claims and litigation and whether those claims will be covered or not under EPLI policies. Stay tuned for continuing developments.

Additional Items of Interest
By: Michelle Dougherty

City of Old Town v. Am. Employers Ins. Co., 858 F. Supp. 264 (D.Me. 1994).

Gerry Perdue was the Chief Building Engineer for Centrum GS Limited, ("Centrum") owner of the Centrum Building. Brenda Brushaber is the General Manager of the Centrum Building and is employed by Steiner & Associates, Inc. ("Associates"), the property manager of the Centrum Building. Perdue's employment was terminated. After his termination, Perdue filed suit against various defendants alleging wrongful termination, intentional infliction of emotional distress, libel, slander, invasion of privacy, fraud, negligence and breach of contract. Perdue specifically alleged that after his wrongful termination, his employer hired eight uniformed police officers to patrol the building's lobby and parking garage and circulated "WANTED POSTERS" of Perdue. The "WANTED POSTERS", which included Perdue's name, home address, driver's license number, social security number and car tag number, were circulated to the public and requested anyone who saw him to call security. Perdue also alleged that defamatory statements were made about him.

Centrum's insurer, St. Paul Guardian Insurance Company ("St. Paul"), filed an action seeking declaratory judgment that it had no duty to defend or indemnify Centrum or any other defendant because Perdue's claims are not covered under the Commercial General Liability policy ("CGL policy") issued to Centrum. The personal injury provisions of the CGL policy stated that coverage is provided for damages for personal injuries that result from the insured's business activities and are caused by a personal injury offense. The District Court found that the personal injury offenses of invasion of privacy and slander did not result from a "business activity" and that St. Paul had no duty to defend. On appeal, however, the Court found that the personal injury offense of invasion of privacy was undertaken by Brushaber as a party of the "business activity" of property management of the Centrum Building to protect the tenants and real estate on behalf of Centrum and is thereby covered under the CGL policy. The case was remanded for decision on the merits regarding a late notice defense.

Gauntlett v. Illinois Union Ins. Co., 2012 U.S. Dist. LEXIS 131086 (N.D. Cal. Sept. 13, 2012).

Illinois Union Insurance Company ("Illinois Union") denied that it had a duty to defend under an Employee Practices Liability Policy issued to David A. Gauntlett, a sole proprietor, wage and hour claims made by an employee. The employee alleged that Gauntlett mis-classified her as an exempt employee and, upon her determination that she was a non-exempt employee; she demanded Gauntlett pay all unpaid overtime wages to which she was entitled. Subsequent to this demand to Gauntlett, she learned that all of her stored email communications had been deleted and her settings changed. Having received no response to her demand for unpaid overtime wages, she resigned. Gauntlett responded to her resignation with a denial that she was entitled to overtime wages. The employee then filed suit stating five causes of action: (1) Failure to pay overtime wages; (2) Failure to pay wages of terminated or resigned employees; (3) Failure to provide restroom breaks and meal periods; (4) Failure to comply with Itemized Employee Wage Statement Provisions; and (5) Violations of the Unfair Competition Law.

Gauntlett provided notice of the claim to Illinois Union and requested a defense. Illinois Union declined coverage. Gauntlett defended the employee claim which was resolved by settlement. Gauntlett then filed a declaratory judgment action seeking to establish that Illinois Union had a duty to defend Gauntlett in the underlying employee action. Pursuant to a motion for summary judgment, the Court denied coverage because the employee claims were based on wage and hour claims which were specifically excluded by the policy language. However, Gauntlett and Illinois Union disputed whether the underlying complaint that someone had logged into the employee's computer, manipulated the settings, and deleted 3,000 emails from her work computer raised allegations that potentially supported a claim for invasion of privacy, which would have been covered under the policy language for "Employment related libel, slander, defamation of character or **any invasion of right of privacy of an Employee**…" California courts have interpreted "any invasion of a right of privacy" to refer to common law torts involving the invasion of a right of privacy. The Court found that the employee's Complaint did not allege that her email communications had been searched, that the communications were personal or that she had a reasonable expectation of privacy in the contents of the deleted emails, nor did she allege that she was offended or suffered any mental anguish or any other damage. The Court further held that the allegation alone that 3,000 emails were deleted did not raise a potential that a violation of the right of privacy was being asserted.

Under California law, an insurer has a duty to defend if the Complaint alleges or if the insurer becomes aware of facts giving rise to the potential for coverage under the insurance policy. The Court concluded that the employee's Complaint did not allege facts to support a potential claim of invasion of a right to privacy and that Gauntlett did not provide extrinsic evidence known to Illinois Union that would reveal a possibility of a privacy claim.

Big 5 Sporting Goods Corp. v. Zurich Am. Ins. Co. & Hartford Fire Ins. Co., 2013 U.S. Dist. LEXIS 100757 (C.D. Cal. July 10, 2013).

Big 5 Sporting Goods Corporation ("Big 5") filed a Complaint against Zurich American Insurance Company ("Zurich") and Hartford Fire Insurance Company ("Hartford"), seeking, among other claims, declaratory judgment on the availability of coverage under Zurich's and Hartford's Commercial General Liability policies ("CGL policies") issued to Big 5 and the carriers' duty to reimburse defense expenses.

Eleven class action lawsuits, filed in 2008 and 2011, were filed against Big 5 alleging that Big 5 infringed on privacy rights by requesting, recording and publishing customer zip codes during credit card transactions in violation of the Song-Beverly Act, a California state statute. The Song-Beverly Act prohibits a corporation that accepts credit cards for business transactions from requesting that the card holder provide "personal identification information" which includes customer zip codes.

The Zurich policy provided coverage for "bodily injury" or "property damage" caused by an "occurrence." It also provided coverage for "personal and advertising injury liability" which included "publication, in any manner, of material that violates a person's right of privacy." However, the Zurich policy also contained statutory violation exclusions barring coverage for bodily injury, property damage and personal and advertising injury "arising directly or indirectly out of Big 5's violation of statutes, particularly statutes which prohibit or limit the distribution, transmission, communication, or sending of information."

The Hartford policy provided coverage for lawsuits for "damages because of 'personal and advertising injury,'" including "oral, written or electronic publication of material that violates a person's right of privacy." The Hartford policy also includes exclusions for "Knowing Violations of Rights of Another," "Right of Privacy Created By Statute," and "Distribution Of Material in Violation Of Statutes."

Under California law, an insurer has a duty to defend if the Complaint alleges or if the insurer becomes aware of facts giving rise to the potential for coverage under the insurance policy. However, if the Complaint does not and can not raise an issue which could bring a claim within the policy coverage, the insurer is not required to defend. Additionally, if extrinsic facts eliminate the potential for coverage, the insurer can decide not to defend even if the allegations in the Complaint indicate potential liability. Further, "[i]nsurance policies are written in two parts: an insuring agreement which defines the type of risks being covered, and exclusions, which remove coverage for certain risks which are initially within the insuring clause." *Rosen v. Nationals Title Insurance Co.*, 56 Cal. App. 4th 1489, 1497, 66 Cal. Rptr. 2d 714 (1997).

The legislative history of the Song-Beverly Act showed that there was no prior common law invasion of privacy right that prevented businesses from requiring customers to provide "personal identification information," including zip codes, in connection with credit card transactions. The Court found that because the "specific and narrow privacy right was expressly created by statute, and therefore not based on common law…any claims alleged in the [underlying class actions] are subject to the relevant statutory exclusions."

The Court held "[i]n sum, because all of the Underlying Actions in [the *Big 5*] case arise out of the alleged violation of the statutory right to privacy, specifically the Song-Beverly Act, coverage is barred by the Statutory Violations Exclusions under the [Zurich and Hartford] Policies. [Zurich and Hartford] have established, as a matter of law, that there is no conceivable theory under which the claims in the Underlying Actions warrant coverage.

Fast Facts about Steptoe & Johnson

More than 300 attorneys

14 Offices in Colorado, Kentucky, Ohio, Pennsylvania, Texas and West Virginia

Over 40 areas of practice

200 attorneys and 200 paraprofessionals serving the energy industry

12th largest energy law practice in the country - Energy Law 360

Top listed in the U.S. in Oil and Gas Law by The Best Lawyers in America®

Top listed in the U.S. in Professional Malpractice by The Best Lawyers in America®

Top listed firm in Ohio, Pennsylvania and West Virginia in a combination of areas by The Best Lawyers in America®

Two Fellows of the American College of Trial Lawyers

Three Fellows of the American College of Labor & Employment Lawyers

AV peer-review rated by Martindale-Hubbell, the highest ranking given

90 lawyers recognized in The Best Lawyers in America®

Follow us on Facebook, Linkedin and Twitter

Steptoe & Johnson PLLC's First Party Team

Team Leaders

Melanie Morgan Norris, *Of Counsel* — Wheeling
304.231.0460 — melanie.norris@steptoe-johnson.com

Michelle E. Piziak, *Of Counsel* — Charleston
304.353.8126 — michelle.piziak@steptoe-johnson.com

Team Members

Laurie C. Barbe, *Member* — Morgantown
304.598.8113 — laurie.barbe@steptoe-johnson.com

Bridget M. Cohee, *Member* — Martinsburg
304.262.3538 — bridget.cohee@steptoe-johnson.com

Michelle Lee Dougherty, *Member* — Wheeling
304.231.0442 — michelle.dougherty@steptoe-johnson.com

Tracey B. Eberling, *Member* — Martinsburg
304.262.3532 — tracey.eberling@steptoe-johnson.com

Eric J. Hulett, *Member* — Martinsburg
304.262.3519 — eric.hulett@steptoe-johnson.com

Lucien G. Lewin, *Member* — Martinsburg
304.262.3528 — lucien.lewin@steptoe-johnson.com

Ancil G. Ramey, *Member* — Huntington
304.526.8133 — ancil.ramey@steptoe-johnson.com

Monté L. Williams, *Member* — Morgantown
304.598.8142 — monte.williams@steptoe-johnson.com

James M. Wilson, *Member* — Bridgeport
304.933.8153 — james.wilson@steptoe-johnson.com

Richard M. Yurko, Jr., *Member* — Bridgeport
304.933.8103 — richard.yurko@steptoe-johnson.com

Hannah Curry Ramey, *Of Counsel* — Huntington
304.526.8132 — hannah.ramey@steptoe-johnson.com

Jason P. Foster, *Associate* — Charleston
304.353.8130 — jason.foster@steptoe-johnson.com

Carlie M. Lacy *Associate* — Morgantown
304.598.8152 — carlie.lacy@steptoe-johnson.com