

The Ethical Investigation of Fidelity Claims: Protecting Privacy

*Andrew F. Caplan
Robert J. Donovan*

I. Introduction

A new fidelity claim hits your desk. The insured asserts that a dishonest employee embezzled millions of dollars. The proof of loss alleges that the dishonest employee and outside confederates funneled money out of the insured's coffers and into accounts held by several outside entities that the confederates controlled. There is much to investigate in order to evaluate the claim.

You immediately roll up your sleeves and get to work. After years of experience investigating fidelity losses, you know the drill. Naturally you have read, and re-read, the key articles concerning the investigation of fidelity claims.¹ It is time to send the insured a set of Inquiries and Requests for information and documentation.²

First on the list of Inquiries and Requests are copies of all documents that reflect the transactions at issue. In a fidelity claim involving an alleged illegal or improper loan to one or more of the bank's customers, the insurer usually will request, among other things, copies of loan files, both for the loans in question and other loans the employee may have made.³ Given the candid comments that often appear in e-mail, you will want to see copies of all e-mails between the principal and the alleged confederates.⁴ E-mail may help determine whether the transactions between the principal and the alleged

¹ See, e.g., Michael Keeley & Sean Duffy, *Investigating the Employee Dishonesty Claim: Interviewing Witnesses, Obtaining Documents, and Other Important Issues*, in *HANDLING FIDELITY BOND CLAIMS* 151-217 (Michael Keeley & Timothy M. Sukel, eds. 1999); James A. Black, Jr., *Managing the Insurer's Response to the Claim*, in *FINANCIAL INSTITUTION BONDS* 575-594 (Duncan L. Clore, ed. 1998); Dolores A. Parr, Donald R. Pratt, Jr., Ronald G. Mund & David J. Krebs, *Investigation of Fidelity Claims and Development of Relevant Facts* (unpublished article presented at the Mid-Winter Meeting of the Fidelity and Surety Committee of TIPS in New York, NY on Jan. 24, 2002) (on file with author).

² Inquiries and Requests are known as "I&Rs" to the cognoscenti. For the origin of the term "Inquiries and Requests," see Keeley and Duffy, *supra* note 1, at 157 n.4.

³ *Id.* at 166.

Loan files may shed light on the following issues: (1) when the loan was extended; (2) who made the loan; (3) who else had knowledge of the loan; (4) whether the loan was approved by the loan committee; and (5) whether the loan was secured properly. Scott D. Baron, *The Fidelity Loss Investigation in a Regulated Industry*, *THE BRIEF* 13, 17 (Spring 1999).

⁴ E-mails preserve statements that often are communicated with the candor of oral conversation. See Mark S. Dichter & Michael S. Burkhardt, *Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in The Internet Age* (June 1999).

Andrew F. Caplan is a partner with Perkins Smith & Cohen LLP in Boston, Massachusetts. Robert J. Donovan is an Operations AVP & Manager, Fidelity/Crime Claims with Factory Mutual Insurance Company in Norwood, Massachusetts.

confederates involved dishonest or fraudulent conduct or merely poor business judgment. The Requests also will seek the personnel file of the accused employee and any confederates. Among other things, personnel records may reveal that the insured had prior knowledge of dishonesty by the accused employee, thereby terminating its fidelity coverage with respect to that employee. Your fingers fly across the keyboard as you type your Inquiries and Requests.

The full story probably cannot be ascertained solely from the documents. You look in your calendar for open dates to interview the insured's employees and others who may be able to shed light on the accusations in the proof of loss.

A nagging doubt creeps into your mind. Are there any privacy laws that forbid disclosure of the documents you plan to request? You pause before you sign and mail the letter. You wonder whether you're asking the insured to breach any privacy rights. Is the insured duty bound to maintain the confidentiality of its records? What are the current rules for workplace privacy?

Is it prudent to show a copy of the proof of loss to individuals who are interviewed in the course of an investigation? There is little doubt about the utility of allowing co-workers and other knowledgeable individuals to review and comment upon the insured's accusations. Will such limited dissemination of the proof of loss subject the investigator to liability for invasion of privacy?

Perhaps you know a little something about privacy law, and you realize there are several different types of privacy torts, each with its own elements. Unless you sleep with the Restatement (Second) of Torts under your pillow, however, you have a host of unanswered questions about the right of privacy. What are the various types of privacy rights? What are the elements of these rights? Doubtless it would help to have a handle on applicable state common law privacy rights before you proceed.

Then there's federal law. Even a causal follower of current events knows that the regulation of privacy is evolving to adapt to modern technology and concerns.⁵ Wasn't it just a few years ago that Congress overhauled banking regulation and enacted privacy safeguards with the passage of the Gramm-Leach-Bliley Act? How does this new legislation affect an insurer's ability to obtain bank documents needed to investigate a financial institution bond claim? You wonder how wiretapping laws apply to modern technologies including e-mail, voicemail and computers. Do citizens have a reasonable expectation of privacy in their e-mail accounts?

⁵ As described by one commentary: "The privacy landscape continues to be a fluid minefield as financial institutions continually face new compliance challenges at the federal, state, and local levels." Elizabeth A. Huber & Elena A. Lovoy, *Update on State Consumer Financial Privacy Legislation and Regulation*, 59 BUS. LAW. 1227, 1227 (May 2004).

The authors of this article are not the first commentators to caution fidelity investigators to be sensitive to privacy and confidentiality rights.⁶ Previous fidelity articles have noted that access to banking data has become more restrictive in light of expanding regulatory restrictions as well as confidentiality and privacy laws.⁷ The insured and its counsel probably are aware of the various privacy rights of the insured's customers, but may not have as much familiarity with the circumstances under which the insured is protected in providing information to its insurer in connection with a fidelity claim.⁸ The insured may have legitimate concerns about protecting privileges or confidentiality in responding to a fidelity insurer's request for documents.⁹ Consequently, after determining what documentation is needed, a fidelity claim investigator must know how to get it.¹⁰ To be successful, a fidelity investigator should be prepared to address and allay the insured's concerns about maintaining privacy and confidentiality.¹¹

This article is intended to help fidelity practitioners spot privacy issues raised by fidelity investigations. The article provides an overview of the major sources of privacy law.¹² It also identifies legal resources to answer specific questions that may arise in fidelity claim investigations.

Section II briefly outlines the history of privacy law in America. Section III addresses the state common law tort of invasion of privacy. Section IV summarizes pertinent federal privacy statutes.

⁶ See, e.g., Patricia H. Thompson, *An Insured's Guide to Effective Claims Investigation, Presentation, and Resolution*, in FINANCIAL INSTITUTION BONDS 533, 559-60 (Duncan L. Clore, ed. 1998); Keeley & Duffy, *supra* note 1, at 165-167; Baron, *supra* note 3, at 13.

⁷ Keeley & Duffy, *supra* note 1, at 165-67; John C. Eichman, *Submission of the Insured's Claim*, in HANDLING FIDELITY BOND CLAIMS 53, 77-78 (Michael Keeley & Timothy M. Sukel, eds. 1999).

⁸ Thompson, *supra* note 6, at 559.

⁹ Keeley & Duffy, *supra* note 1, at 166; Baron, *supra* note 3, at 13 (insured is between proverbial rock and hard place, finding itself under contractual duty to cooperate and produce requested documents, on one hand, while under legal obligation to comply with federal and state banking regulations, privacy laws, the attorney-client privilege, the work product doctrine, and other confidentiality concerns, all of which may prohibit or limit the extent to which insured may voluntarily disclose information); see also Eichman, *supra* note 7, at 77-78.

¹⁰ Keeley & Duffy, *supra* note 1, at 165.

¹¹ Thompson, *supra* note 6, at 559-60.

¹² The article focuses on key elements of privacy laws and omits details in an effort to keep to a reasonable length. The reader should come away with a "lay of the land" but will need to consult other sources to find definitive answers to the myriad of privacy issues that may arise.

II. Origins of Privacy Law

A. THEORETICAL ORIGINS

1. Definition of Privacy and “Right to Privacy”

No definition of privacy is universally accepted.¹³ Courts have long acknowledged the difficulty of defining the right of privacy.¹⁴ One scholar has opined that “privacy relates to the diverse modes by which people, personal information, certain personal property, and personal decision-making can be made less accessible to others.”¹⁵

The right to privacy traditionally has been defined as “the right to be let alone.”¹⁶ A more contemporary definition is “the claim that society is obligated to adopt laws and promote practices that shield against unwanted intrusion, disclosures, publicity, and interference with matters of personal decision-making, identity and conscience.”¹⁷

2. Privacy Rights Are Not Absolute

It is widely understood that privacy rights are not absolute. Courts commonly balance privacy interests against other societal interests including law enforcement, public health, national security, business, efficiency, and the public’s right to know.¹⁸ As often happens in times of national crisis, in the post-9/11 era, the balance increasingly is being struck in favor of security and against privacy.¹⁹

B. Constitutional Origins

The federal Constitution has bestowed federal protection of privacy upon Americans since our nation’s founding.²⁰ While the word “privacy” does not appear in the U.S. Constitution, the Supreme Court has interpreted five of the ten original Bill of Rights guarantees and the Fourteenth Amendment as protective of privacy.²¹

¹³ Anita L. Allen, *Origins and Growth of U.S. Privacy Law*, in 1 FIFTH ANNUAL INSTITUTE ON PRIVACY LAW: NEW DEVELOPMENTS & COMPLIANCE ISSUES IN A SECURITY-CONSCIOUS WORLD 51, 56 (2004).

¹⁴ In 1940, the Massachusetts Supreme Judicial Court observed: “Great difficulty exists in defining a right of privacy that will protect individuals against abuse and yet will not infringe the right of the public and the press to discuss personalities.” *Themo v. New Eng. Newspaper Pub. Co.*, 27 N.E.2d 753 (Mass. 1940).

¹⁵ Allen, *supra* note 13, at 56.

¹⁶ Samuel D. Warren & Louis D. Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193 (1890).

¹⁷ Allen, *supra* note 13, at 56.

¹⁸ *Id.* at 58.

¹⁹ Clare M. Sproule, *The Effect of the USA Patriot Act on Workplace Privacy*, in THE PRACTICAL LAWYER 35, 35-46 (Feb. 2003); see Mark D. Robins, *The Rights of Privacy and Publicity Under Massachusetts Law*, 86 MASS. L. REV. 131, 131 (Spring 2002).

²⁰ Allen, *supra* note 13, at 59.

²¹ *Id.* at 59-60. These constitutional sources of privacy rights include: the First Amendment, which furthers family and group privacy by guaranteeing freedom of religion and freedom of association; the Third Amendment, which protects physical privacy of private homes against military appropriation; the Fourth Amendment, which protects the physical privacy of the home and personal property, and the

Courts uniformly have interpreted the federal Bill of Rights to protect only from governmental, not private, intrusion. Absent “state action,” courts refuse to find a federal constitutional issue.²² Most state courts likewise limit constitutional claims to suits against “state actors.” Therefore, even if a state constitution expressly protects the right to privacy, most jurisdictions do not allow constitutional claims for invasion of privacy against private-sector actors.²³ While constitutional privacy rights do not, with few exceptions, create a cause of action against private parties, these constitutional principles do affect the development of common law privacy rights.

C. TORT LAW ORIGINS

1. Brandeis

Prior to 1890, no English or American court had ever expressly recognized the existence of the right of privacy, although there were decisions that in retrospect appear to have protected it in one manner or another.²⁴ The concept of a right to privacy as a distinct body of tort law originates with a landmark article in the 1890 edition of *Harvard Law Review* by Samuel Warren and Louis Brandeis.²⁵ Warren and Brandeis argued that the law should recognize the “right to be let alone.” Subsequently, after becoming a U.S. Supreme Court Justice, Brandeis, drawing on his 1890 law review article, called the right

informational privacy of one’s papers, correspondence, conversations and electronic communications, by prohibiting arbitrary search and seizure of persons and property; the Fifth Amendment, which prohibits compulsory self-incrimination, allowing for privacy of thought, belief and perspective; the Ninth Amendment, which protects interests in physical, informational, decisional, and proprietary privacy; and the Fourteenth Amendment (interests in freedom of choice, decisional privacy and freedom to withhold information or limit access to it). *Id.*

²² Daniel J. McCoy, *Recent Privacy Law Developments Affecting the Workplace*, in 1 FIFTH ANNUAL INSTITUTE ON PRIVACY LAW: NEW DEVELOPMENTS & COMPLIANCE ISSUES IN A SECURITY-CONSCIOUS WORLD 435, 444 (2004); see *Cole v. Dow Chem. Co.*, 315 N.W.2d 565, 568 (Mich. Ct. App. 1982) (dismissing employee’s privacy claim for lack of state action).

²³ McCoy, *supra* note 22, at 445-46.

California is a notable exception. The California constitution protects the state’s residents against privacy invasions by public and *private* entities alike. *Hill v. Nat’l Coll. Athletic Ass’n.*, 865 P.2d 633 (Cal. 1994). In California, a plaintiff alleging an invasion of the state constitutional right to privacy must establish each of the following: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) conduct by defendant constituting a serious invasion of privacy. *Id.* at 654-55. Private parties are held to a less demanding standard than state actors, because it is easier to avoid transacting business with private parties than with the government. *Id.* at 655-57.

The state constitutions of Alaska, Arizona, California, Hawaii, Montana, South Carolina, Washington, Massachusetts, and Rhode Island provide a general right to privacy. Scott A. Sundstrom, Note, *You’ve Got Mail! (And the Government Knows It): Applying the Fourth Amendment to Workplace E-Mail Monitoring*, 73 N.Y.U. L. REV. 2064, 2076-77 (1998).

²⁴ RESTATEMENT (SECOND) OF TORTS § 652A cmt. a (1977).

²⁵ Robbins, *supra* note 19, at 132 (citing Samuel D. Warren & Louis D. Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193 (1890)); *Themo v. New Eng. Newspaper Pub. Co.*, 27 N.E.2d 753, 753 (Mass. 1940) (“Ever since the publication in 1890 of an article by Samuel D. Warren and Louis D. Brandeis ..., the so called right of privacy has been under discussion.”).

to be let alone “the most comprehensive of rights and the right most valued by civilized men.”²⁶

As the legal community absorbed Justice Brandeis’ ideas, change slowly began to occur in American privacy jurisprudence. While Warren and Brandeis’ thesis was first rejected in Michigan and New York,²⁷ it was accepted by Georgia in 1905.²⁸ Although Warren and Brandeis had written in terms of a comprehensive interest in privacy, the law never united these interests into a single tort.²⁹ The first *Restatement of Torts* articulated a two-dimensional interest in “not having [one’s] affairs known to others or [one’s] likeness exhibited to the public.”³⁰ By 1960, Professor William Prosser had concluded that invasion of privacy was “not one tort, but a complex of four.”³¹

The existence of a right of privacy now is recognized in some form in every American jurisdiction except Minnesota, which recognized misappropriation as a tort but declined to call it part of privacy law.³² Breach of privacy lawsuits can stem from common law, as well as federal or state statutes. Section II of this article discusses common law privacy rights, and Section III discusses select federal privacy statutes. Appendix A provides a compendium of state privacy statutes.³³

2. Four Modern Privacy Torts³⁴

The four separate privacy torts fashioned by Dean Prosser³⁵ later were recognized by the *Restatement (Second) of Torts*.³⁶ The Second Restatement candidly acknowledged

²⁶ *Olmstead v. U.S.*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting to the Court’s holding (later overturned) that wiretaps were not prohibited by the Fourth Amendment).

²⁷ See *Atkinson v. John E. Doherty & Co.*, 80 N.W. 285 (Mich. 1899); *Roberson v. Rochester Folding Box Co.*, 64 N.E. 442 (N.Y. 1902).

²⁸ RESTATEMENT (SECOND) OF TORTS § 652A cmt. a (1977), citing *Pavesich v. New Eng. Life Ins. Co.*, 50 S.E. 68 (Ga. 1905) (recognizing right to privacy and allowing man whose photograph was used without his consent in an insurance advertisement to assert a right of privacy).

²⁹ *Doe v. Methodist Hosp.*, 690 N.E.2d 681, 684 (Ind. 1997).

³⁰ RESTATEMENT OF TORTS § 867 (1939).

³¹ William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

³² ROBERT ELLIS SMITH, *THE LAW OF PRIVACY EXPLAINED*, § 1.07 (1993); see RESTATEMENT (SECOND) OF TORTS § 652A cmt. c (1977).

³³ A discussion of other state statutes related to aspects of privacy is beyond the scope of this article. For comprehensive citations and descriptions of state and federal laws affecting privacy, surveillance, and data collection, published by PRIVACY JOURNAL, see Robert Ellis Smith, *COMPILATION OF STATE AND FEDERAL PRIVACY LAWS* (2002 and Supp. 2003).

³⁴ For a discussion of the four privacy torts, see Ellis Smith, *supra* note 32.

³⁵ Prosser, *supra* note 31, at 389.

³⁶ RESTATEMENT (SECOND) OF TORTS § 652A-652E establishes the general right of privacy. Section 652A (1) provides: “One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.” Section 652A (2) identifies the four types of privacy torts:

The right of privacy is invaded by

- (a) unreasonable intrusion upon the seclusion of another, as stated in § 652B; or
- (b) appropriation of the other’s name or likeness, as stated in § 652C; or
- (c) unreasonable publicity given to the other’s private life, as stated in § 652D; or
- (d) publicity that unreasonably places the other in a false light before the public, as stated in

§ 652E.

that these invasion of privacy torts address four distinct wrongs that are only tenuously related. They were united only in their common focus on some abstract notion of being left alone.³⁷

III. Common Law Invasion of Privacy

Under common law, privacy torts generally include the following: (1) unreasonable intrusion upon the seclusion of another; (2) appropriation of another's name or likeness; (3) unreasonable publicity given to another's private life; and (4) portrayal of an individual in a false light.³⁸

A. INTRUSION UPON SECLUSION³⁹

One can be held liable for invasion of privacy for intentionally intruding, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns. The intrusion must be "highly offensive to a reasonable person" to be actionable.⁴⁰ This standard is not easily defined and must be decided on a case-by-case basis. The intrusion does not have to be physical. It can be accomplished by technological means, such as wiretapping or videotaping. Publicity is not a necessary element.⁴¹

1. Highly Intrusive

There is no liability unless the interference with the plaintiff's seclusion is a substantial one, of a kind that would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object.⁴² "The intrusive conduct must be such that [the defendant] should have realized that it would be offensive to persons of ordinary sensibilities. It is only where the intrusion has gone beyond the limits of decency that liability accrues."⁴³

Thus there is no liability for knocking at the plaintiff's door, or calling him to the telephone on one occasion or even two or three, to demand payment of a debt.⁴⁴ It is only when the telephone calls are repeated with such persistence and frequency as to amount to hounding the plaintiff, that becomes a substantial burden to his existence, that his privacy is invaded.⁴⁵

Liability may arise when outrageous methods are used to collect information in which one has a legitimate interest. For instance, an employer was held liable to an

³⁷ *Id.* at cmt. b.

³⁸ RESTATEMENT (SECOND) OF TORTS §§ 652A-652E (1977); *see generally* DAVID ELDER, PRIVACY TORTS (2002 and Supp. 2004).

³⁹ *See generally* Elder, *supra* note 38, at 2-1-2-301.

⁴⁰ RESTATEMENT (SECOND) OF TORTS § 652B.

⁴¹ *Id.* at cmt. a, b.

⁴² *Id.* at cmt. d.

⁴³ Karsh v. Baybank FSB, 794 A.2d 763, 773 (N.H. 2002).

⁴⁴ RESTATEMENT (SECOND) OF TORTS § 652B cmt. d. (1977).

⁴⁵ *Id.*

employee found at home “ill” (surrounded by empty alcohol bottles) because the employer hired a locksmith to enter the employee’s home and “catch him in the act.”⁴⁶ An employee subjected to urinalysis prevailed on an invasion of privacy claim because the employer insisted on observing her while she urinated.⁴⁷ A private detective was held to have invaded privacy by renting a room in a house adjoining the plaintiff’s residence, and for two weeks looking into the windows of the plaintiff’s upstairs bedroom through a telescope and taking intimate pictures with a telescopic lens.⁴⁸

2. Invasion

The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself, as when the defendant forces his way into the plaintiff’s room in a hotel or insists over the plaintiff’s objection on entering his home.⁴⁹ It also may be by use of the defendant’s senses, with or without mechanical aids, to oversee or overhear the plaintiff’s private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires.⁵⁰ It may be by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, or examining his private bank account.⁵¹ The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of the photograph or information outlined.⁵²

⁴⁶ *Love v. S. Bell Tel. & Tel. Co.*, 263 So. 2d 460 (La. Ct. App. 1972).

⁴⁷ *Kelley v. Schlumberger Tech. Corp.*, 849 F.2d 41 (1st Cir. 1988).

⁴⁸ *Souder v. Pendleton Detectives*, 88 So. 2d 716 (La. Ct. App. 1956); *see also Rhodes v. Graham*, 37 S.W.2d 46 (Ky. 1931) (invasion of privacy by private investigator who tapped plaintiff’s telephone wires and installed a recording device to make a record of plaintiff’s conversations).

⁴⁹ RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977).

⁵⁰ *Id.*; *see, e.g., Karsh v. Baybank FSB*, 794 A.2d 763, 773 (N.H. 2002) (intrusion is not limited to a physical invasion of the plaintiff’s home, room, or quarters, but has been extended to eavesdropping upon private conversations by means of wire tapping and microphones.). Of course, the result can differ under circumstances in which the plaintiff has no reasonable expectation of privacy. *See, e.g., Schmidt v. Devino*, 206 F. Supp. 2d 301, 310 (D. Conn. 2001) (employer who allegedly wiretapped employee’s workplace phone held not liable on common-law claim of invasion of privacy where employee was required to keep office door opened and he believed that secretary outside door was monitoring calls, and, therefore, employee had no reasonable expectation of privacy. Employer held liable under state and federal wiretapping statutes.).

⁵¹ RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977); *see, e.g., Birnbaum v. U.S.*, 588 F.2d 319, 326 (2d Cir. 1978) (recognizing state law claim against a private person for intrusion of privacy based on opening and reading sealed mail); *Vernars v. Young*, 539 F.2d 966, 969 (3d Cir. 1976) (recognizing cause of action and indicating private individuals have a “reasonable expectation that their personal mail will not be opened and read by unauthorized persons”); *Doe v. Kohn, Nast & Graf, P.C.*, 866 F. Supp. 190, 195-96 (E.D. Pa. 1994) (indicating “an employer is not authorized to open mail addressed to a person at his workplace that appears to be personal[.]” and reasonable minds could differ as to whether intrusion occurred when letters were opened, copied and retained) (citation omitted); *Roth v. Farmer-Bocken Co.*, 667 N.W.2d 651 (S.D. 2003) (upholding judgment for plaintiff against former employer for intrusion upon seclusion, where another employee opened envelope addressed to plaintiff, realized it was from a law firm and meant for plaintiff, personally, yet he read the entire contents of the package, and disseminated the materials to his superior).

⁵² RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977).

3. Private/Public

Determining whether an intrusion is unacceptably offensive turns on one's reasonable expectation of privacy.⁵³ "A 'reasonable person' cannot conclude that an intrusion is 'highly offensive' when the actor intrudes into an area in which the victim has either a limited or no expectation of privacy."⁵⁴ "Expectations of privacy are established by general social norms."⁵⁵

There generally is no liability for intrusions into public matters.⁵⁶ For liability to arise, there must be an intrusion either into a private place or a private seclusion that the plaintiff has thrown about his person or affairs.⁵⁷ Thus, there is no liability for examining a public record concerning the plaintiff, or documents that the plaintiff is required to keep and make available for public inspection.⁵⁸ Nor is there liability for observing him or even taking his photograph while he is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye.⁵⁹ Even in a public place, however, there may be some matters about the plaintiff that are not exhibited to the public gaze; and there still may be invasion of privacy when there is intrusion upon these matters.⁶⁰

One court held in a divorce action that the wife did not commit the tort of intrusion into seclusion by accessing her husband's e-mail, since the husband could have no reasonable expectation of privacy as to the files he kept on the family computer, which was located in the sunroom of the marital residence and was used by the entire family.⁶¹ A bank generally should not be held liable for invasion of privacy for providing copies of surveillance videotapes showing customers transacting business at bank.⁶²

B. RIGHT OF PUBLICITY⁶³

The right of publicity imposes liability on one who "appropriates to his own use or benefit the name or likeness of another."⁶⁴ The common form of invasion of privacy based on the right of publicity is the appropriation and use of the plaintiff's name or likeness to advertise the defendant's business or product, or for some similar commercial

⁵³ White v. White, 781 A.2d 85, 91-92 (N.J. Super. Ct. Ch. Div. 2001).

⁵⁴ *Id.* at 92.

⁵⁵ *Id.* at 92, quoting State v. Hempele, 576 A.2d 793 (N.J. 1990).

⁵⁶ RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977).

⁵⁷ *Id.*

⁵⁸ *Id.*

⁵⁹ *Id.*; See, e.g., Key v. Compass Bank, Inc., 826 So. 2d 159 (Ala. Civ. App. 2002) (summary judgment granted to defendant bank on privacy claims of intrusion into solitude, improper publicity of private facts, and false light, where bank provided copy of videotape of customers to newspaper that published picture with story identifying customers a suspects in check fraud; no expectation of privacy because bank lobby is public place).

⁶⁰ RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977).

⁶¹ White v. White, 781 A.2d 85 (N.J. Super. Ct. Ch. Div. 2001).

⁶² See *Compass Bank, Inc.*, 826 So. 2d at 159.

⁶³ See generally Elder, *supra* note 38, at 6-1-6-173.

⁶⁴ RESTATEMENT (SECOND) OF TORTS § 652C (1977).

purpose.⁶⁵ Apart from statute, however, the claim is not limited to commercial appropriation.⁶⁶ It applies also when the defendant makes use of the plaintiff's name or likeness for his own purposes and benefit, even though the use is not a commercial one and even though the benefit sought to be obtained is not financial.⁶⁷

The right of publicity protects the interest of the individual in the exclusive use of his own identity, insofar as it is represented by his name or likeness, and insofar as the use may be of benefit to him or to others.⁶⁸ The right is in the nature of a property right.⁶⁹

Unscrupulous investigative techniques may give rise to liability for violating the right of publicity. For example, the right of publicity may be violated when a private detective impersonates an individual in order to induce third persons to disclose confidential information about the individual that they would not otherwise have disclosed.⁷⁰

C. PUBLIC DISCLOSURE OF PRIVATE FACTS⁷¹

One who publicizes a matter concerning the private life of another is subject to liability for invasion of his or her privacy, if the matter publicized "would be highly offensive to a reasonable person" and "is not of legitimate concern to the public."⁷² Liability depends upon "publicity" given to the private life of the individual.⁷³

1. Publicity

"Publicity" means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge.⁷⁴ It is not an invasion of this right of privacy to communicate a fact concerning the plaintiff's private life to a single person or even to a small group of persons.⁷⁵ On the other hand, any publication in a newspaper or a magazine, even of small circulation, or in a handbill distributed to a large number of persons, or any broadcast over the radio, or a statement made in an address to a large

⁶⁵ RESTATEMENT (SECOND) OF TORTS § 652C cmt. b (1977). The "seminal case," *Pavesich v. New Eng. Life Ins. Co.*, 50 S.E. 68 (Ga. 1905), held an insurer liable for violating the right of publicity for using a picture of plaintiff's likeness, without his consent, in a newspaper advertisement promoting life insurance and contended the words above the picture endorsing the insurance were false and libelous.

⁶⁶ RESTATEMENT (SECOND) OF TORTS § 652C cmt. b (1977).

⁶⁷ *Id.*

⁶⁸ *Id.* at cmt. a.

⁶⁹ *Id.*

⁷⁰ *Id.* at cmt. a, illus. 1; *Goodyear Tire & Rubber Co. v. Vandergriff*, 184 S.E. 452 (Ga. Ct. App. 1936).

⁷¹ See generally Elder, *supra* note 38.

⁷² RESTATEMENT (SECOND) OF TORTS § 652D (1977).

⁷³ *Id.* at cmt. a.

⁷⁴ *Id.*

⁷⁵ *Id.*

audience, is sufficient to give publicity within the meaning of the term as it is used in this Section.⁷⁶

2. Private Matters

The right of publicity applies only to publicity given to matters concerning the private, as distinguished from the public, life of the individual.⁷⁷ There is no liability when the defendant merely gives further publicity to information about the plaintiff that already is public.⁷⁸ Similarly, there is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye.⁷⁹ Thus he normally cannot complain when his photograph is taken while he is walking down the public street and is published in the defendant's newspaper.⁸⁰ Nor is his privacy invaded when the defendant gives publicity to a business or activity in which the plaintiff is engaged in dealing with the public.⁸¹

On the other hand, when a photograph is taken without the plaintiff's consent in a private place, or one already made is stolen from his home, the plaintiff's appearance that is made public when the picture appears in a newspaper still is a private matter, and his privacy is invaded.⁸²

3. Highly Offensive

This claim gives protection only against unreasonable publicity, of a kind highly offensive to the ordinary reasonable man.⁸³ The tort does not aim to provide complete privacy, and one must expect and endure the ordinary incidents of community life.⁸⁴ This tort does not protect against casual observations by one's neighbors of one's comings and goings or ordinary daily activities, nor does it shield against such matters being described in the press as a matter of casual interest to others. As a matter both of the common law of torts and First Amendment freedom of the press, an action for invasion of privacy cannot be maintained when the subject-matter of the publicity is a matter of "legitimate concern to the public."⁸⁵

⁷⁶ *Id.*

⁷⁷ *Id.* at cmt. b.

⁷⁸ *Id.*

⁷⁹ *Id.*

⁸⁰ *Id.*

⁸¹ *Id.*

⁸² *Id.*

⁸³ *Id.* at cmt. c.

⁸⁴ *Id.*

⁸⁵ *Id.* at cmt. d, (citing *Cox Broadcasting Co. v. Cohn*, 420 U.S. 469 (1975) (under the First Amendment, there can be no recovery for disclosure of, and publicity to, facts that are a matter of public record)).

It has not been established with certainty that liability for public disclosure of private facts is consistent with the free-speech and free-press provisions of the First Amendment to the Constitution, as applied to state law through the Fourteenth Amendment. RESTATEMENT (SECOND) OF TORTS § 652D Special Note on Relation of § 652D to the First Amendment to the Constitution. In light of the Supreme Court's First Amendment jurisprudence, it is unsettled whether liability can constitutionally be imposed for

By way of illustration, an employer in Utah did not invade the privacy of an employee, when, in the course of a security investigation, it showed several people a videotape of the employee being sexually assaulted, even though others (including the plaintiff's immediate supervisor) could see the video while walking out of the security office.⁸⁶

D. FALSE LIGHT PUBLICITY⁸⁷

False light publicity is the publication of facts that place a person in a false light even though the facts themselves may not be defamatory.⁸⁸ To be actionable, the false light must be "highly offensive to a reasonable person."⁸⁹ In addition, the actor must have knowledge of or act in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.⁹⁰ The false light tort, like public disclosure of private facts, discussed above, is limited to situations where the plaintiff is given "publicity."⁹¹

The interest protected by a false light claim is the interest of the individual not to appear before the public in an objectionable false light or false position, or in other words, otherwise than as he is.⁹² "False light" tends to fare poorly, even in those jurisdictions that recognize the tort.⁹³

False light applies only when the publicity given to the plaintiff has placed him in a false light before the public, of a kind that would be highly offensive to a reasonable person.⁹⁴ In other words, it applies only when the defendant knows that the plaintiff, as a reasonable man, would be justified in the eyes of the community in feeling seriously offended and aggrieved by the publicity.⁹⁵ The plaintiff's privacy is not invaded when the unimportant false statements are made, even when they are made deliberately.⁹⁶ It is only when there is such a major misrepresentation of his character, history, activities or

private facts that would be highly offensive to a reasonable person and that are not of legitimate public concern. *Id.*, citing *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964) and *Cox Broadcasting Co. v. Cohn*, 420 U.S. 469 (1975). See *Uranga v. Federated Publ'ns, Inc.*, 67 P.3d 29 (Idaho 2003).

⁸⁶ *Shattuck-Owen v. Snowbird Corp.*, 16 P.3d 555 (Utah 2000).

⁸⁷ See generally *Elder*, *supra* note 38, at 4-1-4-170.

⁸⁸ RESTATEMENT (SECOND) OF TORTS § 652E.

⁸⁹ *Id.*

⁹⁰ *Id.*

Unlike defamation, truth is not an affirmative defense to a false-light claim; rather, "falsity" is an element of the plaintiff's claim, on which the plaintiff bears the burden of proof. *Regions Bank v. Plott*, No. 1030436, 2004 Ala. LEXIS 163 (Ala. June 25, 2004) ("falsity is the sine qua non of a false-light claim"). *Id.* at *10.

⁹¹ RESTATEMENT (SECOND) OF TORTS § 652E cmt. a, (citing § 652D cmt. a (1977)). "Publicity" is more difficult to prove than mere "publication," which is an element of a defamation claim. The "publicity" element is not satisfied by the communication of a fact to a single person or even to a small group of persons.

⁹² RESTATEMENT (SECOND) OF TORTS § 652E cmt. b (1977).

⁹³ *McCoy*, *supra* note 22, at 449, n.18, and cases cited.

⁹⁴ RESTATEMENT (SECOND) OF TORTS § 652E cmt. c. (1977).

⁹⁵ *Id.*

⁹⁶ *Id.*

believes that serious offense may reasonably be expected to be taken by a reasonable man in his position, that a cause of action for invasion of privacy exists.⁹⁷

E. EXTENT OF ADOPTION OF PRIVACY TORTS BY STATES

From 1900 to 1990, all states recognized a right to privacy (in a tort action) either by statute or common law, except Minnesota, which recognized misappropriation as a tort but declined to call it part of privacy law.⁹⁸ Resources on privacy rights are listed below.⁹⁹

F. COMMON LAW PRIVACY RIGHTS

The various common law privacy rights have given rise to a small body of case law that may be of interest to fidelity claims investigators. This section discusses common law privacy or confidentiality claims involving (1) workplace investigations, (2) insurance claims investigations, (3) bank records, (4) personnel records, and (5) retaliatory litigation.

1. Workplace Investigations

Given that fidelity claims arise out of dishonest acts by employees, the investigation of such claims may implicate workplace privacy concerns. A fidelity investigator should be careful not to ask an insured employer to gather and submit any materials in a manner that may infringe on an employee's right of workplace privacy.¹⁰⁰ A few points should be kept in mind.

Privacy law generally will allow an employer reasonably to investigate suspected employee misconduct. An employer who questioned an employee "in a reasonable manner and in good faith" about an altered check, for example, did not violate her right to privacy.¹⁰¹

An employer may find itself embroiled in litigation if it accuses an employee of dishonesty. An Oregon employer was required to stand trial to defend against the tort of "outrage" after it accused a department store employee of theft and threatened and overzealously interrogated her in an attempt to force a confession. The Court noted that the employer had undertaken the "cold-blooded tactic of interrogation upon scanty evidence."¹⁰²

⁹⁷ *Id.*

⁹⁸ Smith, *supra* note 32.

⁹⁹ For comprehensive citations and descriptions of state and federal laws affecting privacy, surveillance, and data collection, published by PRIVACY JOURNAL, see Smith, *supra* note 33.

¹⁰⁰ One can imagine an unusual circumstance in which an insured employer submits materials in support of a claim that raise concerns about whether they were gathered in violation of any right of privacy.

¹⁰¹ Cangelosi v. Schwegmann Bros. Grant Supermarkets, 379 So. 2d 836, 838 (La. Ct. App. 1980).

¹⁰² Hall v. May Dep't Stores Co., 637 P.2d 126, 133 (Or. 1981).

It has been recognized that the right of seclusion, among other things, protects an employee from intrusive surveillance by a current or former employer.¹⁰³ It has been held that when an employer informs employees that it could inspect laptops lent to employees for use in the workplace, however, an employee has no right of privacy to the information stored on his or her computer.¹⁰⁴ This notice destroys any reasonable expectation of privacy that employee may have had.¹⁰⁵

Not that there can't be a right of privacy in employer-owned equipment furnished to an employee for use in his place of employment. In the context of whether there is a right to privacy in employer-owned equipment furnished to an employee for use in his place of employment, if the employer equips the employee's office with a safe or file cabinet or other receptacle in which to keep his private papers, he can assume that the contents of the safe are private.¹⁰⁶

An employee's right to e-mail privacy largely is governed by state tort law. The tort most relevant to e-mail interception by employers is the unreasonable intrusion upon the seclusion of another. Courts generally consider electronic surveillance, such as telephone monitoring, an "intrusion" sufficient to satisfy that element of the tort.¹⁰⁷ The critical issues to examine when determining employer tort liability for monitoring or intercepting employee e-mail messages are: (1) does the plaintiff have a reasonable expectation of privacy, and, if so, (2) was there a legitimate business justification for the intrusion sufficient to override that expectation.

An employer's stated policies regarding privacy and appropriate computer use may be decisive in determining the employer's liability for invasion of privacy. For example, employers who do not warn their employees that e-mail is monitored may face liability for such monitoring.¹⁰⁸

¹⁰³ *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743-44 (7th Cir. 2002) (holding that the plaintiff stated a cognizable intrusion upon seclusion claim by alleging in complaint that defendant former employer, "without right or cause, hired Investigative Associates, a private agency, to perform surveillance on the Plaintiff, even though he was no longer in the Defendant's employ, thereby violating his common-law Right to Privacy by invading his seclusion.").

¹⁰⁴ *Id.* at 743.

¹⁰⁵ As explained by Judge Posner of the Seventh Circuit Court of Appeals:

The laptops were [the employer's] property and it could attach whatever conditions to their use it wanted to. They didn't have to be reasonable conditions; but the abuse of access to workplace computers is so common (workers being prone to use them as media of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible.

Id.

¹⁰⁶ *Id.*

¹⁰⁷ *See, e.g., Billings v. Atkinson*, 489 S.W.2d 858 (Tex. 1973); *Nader v. Gen. Motors*, 255 N.E.2d 765 (N.Y. 1970).

¹⁰⁸ *Restuccia v. Burk Tech.*, No. 95-2125, 1996 Mass. Super. Lexis. 367 (Aug. 13, 1996) (holding that interception of e-mail communications was arguably an invasion of privacy under Massachusetts statutory privacy law; court noted that employees had not been warned that e-mail was monitored).

In *Smyth v. Pillsbury Co.*,¹⁰⁹ however, the court held that *even in the absence* of a company e-mail policy, plaintiffs would not have had a reasonable expectation of privacy in their work e-mail:

Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost. Significantly, the defendant did not require plaintiff, as in the case of urinalysis or personal property search to disclose any personal information about himself. Rather, plaintiff voluntarily communicated the alleged unprofessional comments over the company e-mail system. We find no privacy interests in such communications.¹¹⁰

Further, even if an employee had a reasonable expectation of privacy in his or her work e-mail, a defendant's legitimate business interest may trump a plaintiff's privacy interests.¹¹¹ An employer's interest in uncovering employee fraud, and then seeking an insurance recovery for resulting losses, should trump a dishonest employee's purported expectation of privacy in e-mail.

2. Insurance claims investigations

The authors are not aware of any cases applying the intrusion of seclusion tort to a fidelity claim investigation. Cases involving other types of insurance claims investigation may be instructive, however.¹¹²

Obtaining information about an individual only by searching public records and obtaining voluntary interviews with people in the community does not constitute intrusion upon seclusion because such information is not "private."¹¹³ In *Myrick v. Barron*, for example, the Alabama Supreme Court held that a defendant insurer was entitled to judgment as a matter of law on a claim for invasion of privacy and seclusion claim, where the insurer had searched public records and conducted interviews with the plaintiff's acquaintances in an effort to gain information about him.¹¹⁴ The court noted that the plaintiff had not alleged that the defendant "entered his home, searched through his private papers, wiretapped his telephone, . . . eavesdropped on any of his

¹⁰⁹ 914 F. Supp. 97 (E.D. Pa. 1996).

¹¹⁰ *Id.* at 101; *see also* *Garrity v. John Hancock Mut. Life Ins. Co.*, No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002) (employees had no reasonable expectation of privacy where they admitted knowing employer had ability to look at e-mail on company's intranet system, and knew they had to be careful about sending e-mails).

¹¹¹ *Garrity*, 2002 U.S. Dist. LEXIS 8343, at *12.

¹¹² *See generally* J. D. Emerich, Annotation, *Investigations and Surveillance, Shadowing and Trailing, as Violation of Right of Privacy*, 13 A.L.R.3d 1025 (1967 and Supp. 2004).

¹¹³ *Myrick v. Barron*, 820 So. 2d 81, 85-87 (Ala. 2001); *Nader v. Gen. Motors Corp.*, 255 N.E.2d 765 (N.Y. 1970) (no intrusion upon seclusion when defendant interviewed many persons who knew the plaintiff, asking questions about him and casting aspersions on his character).

¹¹⁴ Curiously, the insurer was not investigating a claimant, but rather an influential state senator who refused to support the confirmation of an insurance executive to the Board of Trustees of Auburn University. *Myrick*, 820 So. 2d at 83-84.

conversations . . . [or] obtained private records concerning his business or personal affairs.”¹¹⁵

Similarly, in *York v. General Electric Co.*, the Ohio Court of Appeals found that worker’s compensation insurer did not invade the privacy of a claimant when it hired a surveillance company to investigate whether the plaintiff employee was engaged in any activity inconsistent with his limitations and whether he displayed disability or discomfort in his daily activities.¹¹⁶ The plaintiff employee was videotaped while working in his yard from across the street, while arriving at work, while going to the chiropractor’s office, and while visiting a lawnmower shop.¹¹⁷ The court held that there was no invasion of privacy because the videotape did not depict any private activities of plaintiff employee within his home.¹¹⁸

In *Swarthout v. Mutual Service Life Insurance Co.*, the Minnesota Court of Appeals found that a material fact sufficient to defeat summary judgment on a privacy claim for intrusion on seclusion existed when a life insurer altered a plaintiff applicant’s medical release form to enable it to acquire medical information about the plaintiff from several unauthorized sources and then posted the illicitly obtained information in a medical insurance database.¹¹⁹

Egregious misconduct begets liability. For example, in *Ellis v. Safety Insurance Co.*, an automobile owner who submitted an automobile theft claim established triable issues of fact under the Massachusetts privacy statute¹²⁰ by alleging that an insurance claims adjuster followed her and her mother around Boston in a car on numerous occasions, called her and her mother on the telephone numerous times and asked her: “How can you black people afford this type of expensive car?”¹²¹

¹¹⁵ *Id.* at 87.

¹¹⁶ *York v. Gen. Elec. Co.*, 759 N.E.2d 865 (Ohio Ct. App. 2001).

¹¹⁷ *Id.*

¹¹⁸ *Id.*; accord *Schupmann v. Empire Fire & Marine Ins. Co.*, 689 S.W.2d 101 (Mo. Ct. App. 1985) (an insured failed to state a cause of action against her insurer for invasion of privacy because the insurance investigator’s question to a neighbor was insufficient to constitute an intrusion into the private seclusion around the insured’s affairs).

Similar principles apply when an employer investigates potential employee defalcations. In an action by deputy sheriffs who alleged their privacy was invaded when the sheriff’s department conducted covert video surveillance of the jail office, which had been experiencing unexplained loss of inmates’ money, summary judgment was correctly granted against plaintiffs where they had no reasonable expectation of privacy against being videotaped in the office, where even if the videotaping was intrusive, it could not be considered offensive in that intrusiveness was abated by absence of audio capabilities, objectives of taping were lawful, and the “intrusion” took place in non-private office in booking area of county jailed, wherein plaintiffs had a diminished expectation of privacy. *Sacramento County Deputy Sheriffs’ Assn. v. County of Sacramento*, 59 Cal. Rptr. 2d 834 (Cal. Ct. App. 1996).

¹¹⁹ *Swarthout v. Mut. Serv. Life Ins. Co.*, 632 N.W.2d 741, 745 (Minn. Ct. App. 2001). The court noted: “Use of improper methods to obtain information does not necessarily satisfy the ‘highly offensive’ prong of the intrusion-upon-seclusion analysis where the information in question could be obtained by a different, proper manner.”

¹²⁰ MASS. GEN. LAWS ch. 214 § 1B (2004).

¹²¹ *Ellis v. Safety Ins. Co.*, 672 N.E.2d 979 (Mass. App. Ct. 1996).

3. Bank Records

It is routine to request loan files and other customer records when investigating a financial institution bond claim. Such requests may raise an issue concerning whether the records are confidential or private such that the insured is unwilling to produce the information voluntarily. Financial institutions may be hesitant to produce their customer's records for fear of being sued by the customer for invasion of privacy or breach of confidentiality.

The common law of bank confidentiality has been shaped, at least in part, by the expectation of banks and their customers that banking information will be maintained in confidence.¹²² A number of courts have held, as a matter of state law, that a bank has a duty to keep its customers' records confidential.¹²³ Courts have found such a duty of confidentiality based on various rationales, including: (1) an implicit agreement between a bank and its customer or depositor that no information may be disclosed by a bank concerning the customer or depositor's account, unless authorized by law or by the

¹²² One court suggests that it should be obvious to banks that they must maintain the confidentiality of customer records. *See Peterson v. Idaho First Nat'l Bank*, 367 P.2d 284, 290 (Idaho 1961) ("It is inconceivable that a bank would at any time consider itself at liberty to disclose the intimate details of its depositors' accounts. Inviolate secrecy is one of the inherent and fundamental precepts of the relationship of the bank and its customers or depositors.").

Weighing whether to extend the breach-of-confidence cause of action to banking relationships, the Second Circuit noted:

[M]ost depositors believe banks will keep their banking activities confidential. At the very least, banks have fostered that impression. The American Bankers Association counsels its members that customer account information should generally be kept confidential, and acknowledges that most customers assume that banking transactions are confidential.... [A]ny customer who has ever tried to get his or her own account balance over the phone from an obdurate bank employee would be quite surprised to learn that the same information could be freely disclosed to a law enforcement agency.

Young v. United States Dep't of Justice, 882 F.2d 633, 643-44 (2d Cir. 1989) (internal citations omitted) (abstaining from deciding whether to extend the breach-of-confidence cause of action to banking relationships in light of the lack of New York precedent and concern that if it found no duty requiring New York banks to keep account information confidential, some customers might be inclined to transfer their business from institutions in New York, home to one of the world's financial capitals, to banks in "confidential" jurisdictions).

¹²³ *Burrows v. Superior Court*, 529 P.2d 590 (Cal. 1974); *Barnett Bank of W. Fla. v. Hooper*, 498 So. 2d 923, 925 (Fla. 1986); *Milohnich v. First Nat'l Bank of Miami Springs*, 2244 So. 2d 759, 760-61 (Fla. Ct. App. 1969); *Peterson*, 367 P.2d at 290; *Ind. Nat'l Bank v. Chapman*, 482 N.E.2d 474, 480 (Ind. Ct. App. 1985); *Suburban Trust Co. v. Waller*, 408 A.2d 758, 762-65 (Md. Ct. Spec. App. 1979); *Richfield Bank & Trust Co. v. Sjogren*, 244 N.W.2d 648, 651 (Minn. 1976); *see generally* Roy Elbert Huhs, Jr., *To Disclose or Not to Disclose Customer Records*, 108 BANKING L.J. 30 (1991); Edward L. Raymond, Annotation, *Bank's Liability, Under State Law, for Disclosing Financial Information Concerning Depositor or Customer*, 81 A.L.R.4th 377 (1990 and Supp. 2004); Baron, *supra* note 3, at 18-20.

customer or depositor;¹²⁴ (2) a fiduciary relationship between bank and customer;¹²⁵ and (3) a principal-agent relationship between bank and customer.¹²⁶

Several courts have distinguished between information concerning a customer's deposits or other bank transactions, and other financial information such as loan information, and found that only the former is confidential.¹²⁷ Under this line of authority, "whatever expectations of confidentiality may inhere in the traditional relationship between bank and depositor, such expectations are wholly lacking in the context of the debtor-creditor loan relationship" and, consequently, borrowers have no recognizable confidentiality interest in such records.¹²⁸

Based on the foregoing line of authority, a customer arguably does not have a legitimate expectation of privacy in his or her loan files to the extent that he was party to dishonest activity. "[T]o the extent that there is a implied agreement by the bank to keep its customers' loan records confidential, it should also be implied that the bank may disclose certain records to the extent the customer has engaged in a dishonest or fraudulent scheme and where the bank has an interest in disclosing such scheme."¹²⁹ One commentator has argued that "the bank should always be permitted to disclose to a fidelity insurer information concerning loans to its customers where such loans are the subject of a bond claim."¹³⁰

Some courts do not recognize a distinction between borrowers and depositors, and appear to require banks to maintain both types of customer records in confidence. Even those courts recognize that a bank's general duty of confidentiality concerning a depositor's account is qualified.¹³¹ Some courts allow banks to disclose financial information about customers in four situations (a) where disclosure is under compulsion by law; (b) where there is a duty to the public to disclose; (c) where the interests of the bank require disclosure; or (d) where the disclosure is made with the express or implied consent of the customer.¹³²

¹²⁴ *Peterson*, 367 P.2d at 290.

¹²⁵ *United States v. First Nat'l Bank of Mobile*, 67 F. Supp. 616, 624 (1946), *modified*, 160 F.2d 532 (5th Cir. 1947).

¹²⁶ *Brex v. Smith*, 146 A. 34, 36 (N.J. Ch. 1929). This section focuses on a bank's implied duty of confidentiality and the right of privacy. Claims of breach of fiduciary duty are beyond the scope of this article. See generally *Huhs*, *supra* note 123; see also *Raymond*, *supra* note 123.

¹²⁷ *Young*, 882 F.2d at 643-44; *Hopewell Enters. v. Trustmark Nat'l Bank*, 680 So. 2d 812, 817 (Miss. 1996); *Norkin v. Hoey*, 586 N.Y.S.2d 926, 931 (N.Y. App. Div. 1992); *Graney Dev. Corp. v. Taksen*, 400 N.Y.S.2d 717 (N.Y. Sup. Ct. 1978); (defendant bank loaned plaintiff money and plaintiff defaulted; bank revealed default to prospective lender and seller of property who then declined to complete transaction; held, relationship between bank and plaintiff was solely that of creditor and debtor, not agent and principal; no implied contractual agreement regarding confidentiality), *aff'd*, 411 N.Y.S.2d 756 (N.Y. App. Div. 1978); *Schoneweis v. Dando*, 435 N.W.2d 666 (Neb. 1989).

¹²⁸ *Norkin*, 586 N.Y.S.2d at 930, *citing Graney*, 400 N.Y.S.2d at 717.

¹²⁹ *Baron*, *supra* note 3, at 18.

¹³⁰ *Id.*

¹³¹ See, e.g., *Barnett Bank of W. Fla. v. Hooper*, 498 So. 2d at 923, 925 (Fla. Ct. App. 1969).

¹³² See, e.g., *id.* at 925 (recognizing these four exceptions to the duty of confidentiality and further holding that a bank's duty of confidentiality may also be overridden in other "special circumstances" where

The authors concur with a prior commentator's view that it is in the interest of the bank to disclose customer loan information to the fidelity insurer to the extent the information relates to dishonest activity that is the subject of a bond claim.¹³³ It also is in the public interest for the nation's financial institutions to be able to provide relevant documentation to fidelity insurers in order to recoup losses due to employee defalcations.

Certain courts tightly restrict the circumstances under which a bank is relieved of its implied duty not to disclose customer information. These courts refuse to grant banks the discretion to decide what is or is not in the public interest to disclose, and what is or is not in the best interest of the bank to disclose. Under this line of authority, absent compulsion by law, a bank may not make any disclosures concerning a depositor's account without the express or implied consent of the depositor.¹³⁴

Even if applicable law does not prohibit an insured from disclosing its customers' records, the insured still may be hesitant to do so in order to maintain customer relations or out of an abundance of caution.¹³⁵ The insurer should offer to enter a confidentiality agreement that recognizes that customer records are submitted solely in connection with the bond claim investigation and may not be disclosed to third parties.¹³⁶

4. Personnel Records

Fidelity claim investigators routinely request that the insured employer submit a copy of the personnel file of each employee accused of wrongdoing.¹³⁷ Employers often resist such requests because they think that personnel records are private or confidential and that disclosing their contents may result in employer liability. This section discusses

the bank has a duty of disclosure); *Ind. Nat'l Bank v. Chapman*, 482 N.E.2d 474 (Ind. Ct. App. 1985) (holding that a bank was not liable as a matter of law for invasion of privacy, or for breach of an implied contract, when a loan officer turned over information regarding a customer's automobile loan account to a police officer, without a subpoena or search warrant, who was conducting an arson investigation in which the customer was a suspect), *citing* *Tournier v. Nat'l Provincial & Union Bank of Eng.*, 1 K.B. 461, 473 (1923). *Tournier* is acknowledged as the first known decision recognizing an implied duty of confidentiality owed by a bank to its customer. *Velasquez-Campuzano v. Marfa Nat'l Bank*, 896 F. Supp. 1415, 1426 (W.D. Tex. 1995).

¹³³ Baron, *supra* note 3, at 18.

Further, in balancing the privacy interests of a bank's customers against the bank's self-interest in protecting itself from wrongdoing and society's interest in investigating and apprehending criminals, the customers' interest should give way. *See* *People v. Muchmore*, 154 Cal. Rptr. 488 (Cal. Ct. App. 1979) (rejecting criminal defendant's argument that a bank violated the California Right to Financial Privacy Act, Gov. Code, §§ 7460-7493, when the bank, without notice to defendant, provided copies of his banking records to authorities investigating him for criminal check kiting). "[T]he shield of privacy cannot be used to shelter criminal acts." *Id.*

¹³⁴ *See, e.g.,* *Suburban Trust Co. v. Waller*, 408 A.2d 758 (Md. Ct. Spec. App. 1979); *Burrows v. Superior Court*, 529 P.2d 590 (Cal. 1974); *Peterson v. Idaho First Nat'l Bank*, 367 P.2d 284 (Idaho 1961).

¹³⁵ Baron, *supra* note 3, at 18.

¹³⁶ *Id.*

¹³⁷ *See* *Keeley & Duffy, supra* note 1, at 181-82 (recommending that insurers consider asking the insured to submit a copy of the personnel file of the principal, as well as for other employees involved, in connection with all employee dishonesty claims, and explaining the relevance of such materials to a fidelity investigation).

the privacy of personnel records and the circumstances under which their contents may be revealed to third parties.

No federal statute comprehensively regulates the confidentiality of personnel files of private sector employees.¹³⁸ As such, the issue of whether an employer will incur liability for providing a third party access to the personnel file of a private sector employee are decided under general principles of privacy established by state statutory and common law.¹³⁹

A prima facie case in an intrusion upon seclusion action brought by an employee against his or her employer requires proof that: (1) the employer intentionally intruded upon the solitude or seclusion of the employee in his or her private affairs or concerns; and (2) the intrusion was highly offensive to a reasonable person.¹⁴⁰ The viability of a private employee's claims for invasion of privacy in the workplace turns on: (1) the reasonableness of his or her privacy expectation; and (2) the sufficiency of the employer's business justification for the intrusion.¹⁴¹ Courts addressing such claims balance the employee's privacy expectations against employer's legitimate interests.¹⁴²

¹³⁸ While the Freedom of Information Act, 5 U.S.C. § 552a (2004), and the Privacy Act, 5 U.S.C. § 552b (2004), regulate access to the personnel files of federal employees, and nearly all the states statutorily regulate access to the personnel files of public employees, private sector employees fall outside the ambit of these statutes. *See* Fed. Labor Relations Auth. v. U.S. Dept. of Navy, 966 F.2d 747, 773 (3rd Cir. 1992) (Rosenn, J., dissenting) (describing how the personnel files of federal employees are "protected by the Privacy Act; in the private sector, employees are not so protected").

Note that the prohibition against disclosure of public records that may constitute an "unwarranted invasion of privacy" under the Massachusetts Public Records Act, Mass. Gen. L. ch. 4, § 7, has been held to give public employees greater protection than is afforded by the Massachusetts Privacy Statute, Mass. Gen. L. ch. 214, § 1B. *See* Pottle v. School Comm. of Braintree, 482 N.E.2d 813 (Mass. 1985); *see also* Mass. Gen. L. ch. 4, § 7, Twenty-sixth (c) (expressly exempting "personnel...files or information" from the definition of a public record subject to public disclosure); Joshua M. Davis & Hannah S. Ross, *Privacy in the Workplace: A Defense Perspective*, in 2 MASSACHUSETTS EMPLOYMENT LAW 17-1, 17-2 (John F. Atkins & Nancy S. Shilepsky eds., 2003) (Under the Fourth Amendment of the United States Constitution and Article 14 of the Massachusetts Declaration of Rights, public employees have greater rights of privacy than do those who are not employed in the public sector.)

¹³⁹ *See infra*, Section II; *see generally* Tracy B. Holton, *Cause of Action to Recover Damages for Invasion of Private Sector Employee's Privacy*, 18 CAUSES OF ACTION 2d 87 §§ 3-6 (2003) (collecting cases).

¹⁴⁰ *See infra*, Section II(A).

¹⁴¹ Holton, *supra* note 139, at § 3; *see also* Bratt v. Int'l Bus. Mach. Corp., 467 N.E.2d 126, 126 (Mass. 1984) (In the workplace context, the Massachusetts Privacy Act requires the Court "to balance the employer's legitimate business interest in obtaining and publishing the information against the substantiality of the intrusion on the employee's privacy resulting from the disclosure."); *id.* at 520 ("Legitimate countervailing . . . interests in certain situations may render disclosure of personal information reasonable and not actionable under the statute." *Id.* at 520; Davis & Ross, *supra* note 138, at 17-11 (The Massachusetts personnel records statute, Mass. Gen. L. ch. 149, § 52C, "does not address whether and under what circumstances an employer may disclose information contained in an employee's personnel file to individuals other than the employee. The legality of such a disclosure would thus be determined under the general privacy statute by balancing the employer's business interest in disclosing the information contained in the records against the employee's interest in maintaining his or her confidentiality."))

¹⁴² *See, e.g.*, Fletcher v. Price Chopper Foods of Trumann, Inc., 220 F.3d 871, 878 (8th Cir. 2000) (dismissing employee claim of privacy invasion by employer who legitimately obtained her medical information because of legitimate employer interest in her health status); Bratt, 467 N.E.2d at 126 (holding

In the employment context, a conditional privilege to disclose personal information concerning an employee exists when publication is reasonably necessary to serve legitimate business interests of the employer.¹⁴³ The qualified privilege's protection depends on the claimant's honesty of purpose and the absence of wrongful motive, bad faith, malice, and abuse.¹⁴⁴ So long as there is no malice, it is immaterial whether the qualifiedly privileged communication was true or false.¹⁴⁵ This qualified privilege generally does not extend to invasions of privacy that do not involve publication.¹⁴⁶

Consent, waiver, justification and legal obligation are the employer's principal defenses to liability for invading an employee's privacy.¹⁴⁷ A plaintiff who voluntarily and knowingly consents to a particular intrusion by his or her employer, as evidenced by an employee handbook or other company policy statement, for example, can have no reasonable expectation of privacy.¹⁴⁸ Consent negates liability provided that the invasion

intra-corporate communication of employee's "paranoid" medical diagnosis sufficiently personal and unadorned by countervailing interests to go to jury on question of Mass. Gen. L. ch. 214 § 1B violation (state privacy statute)); *Hasting & Sons Publ'g Co. v. City Treasurer of Lynn*, 375 N.E.2d 299 (Mass. 1978) (holding disclosure of payroll records non-violative of § 1B); *Miller v. Motorola, Inc.*, 202 Ill. App. 3d 976, 560 N.E.2d 900 (1990) (upholding employee claim of invasion of privacy against employer who revealed her surgical procedure to co-employees); *Fallstrom v. L.K. Comstock & Co.*, No. CV 9901525835, 2001 Conn. Super. LEXIS 129, at *19-22 (Jan. 22, 2001) (holding colorable employee claim of invasion of privacy against employer who revealed employee's drug test results to fellow employees); *Battenfield v. Harvard Univ.*, No. 91-5089-F, 1993 Mass. Super. LEXIS 253 (Aug. 31, 1993) (holding that an employee's claim that her employer violated her privacy by disclosing information contained in her personnel file, such as salary and job description, failed under § 1B because it was not a disclosure of facts of a highly personal or intimate nature when there exists no legitimate countervailing interests) (quotation omitted).

¹⁴³ RESTATEMENT (SECOND) OF TORTS § 652G, at 401 (1977) (affording the same qualified privilege available to defendants in defamation cases); Frank J. Cavico, *Invasion Of Privacy In The Private Employment Sector: Tortious And Ethical Aspects*, 30 HOUS. L. REV. 1263, 1281-83 & nn.72-83 (1993), (and authorities cited); *Bratt*, 467 N.E.2d at 131 (identifying a long-standing legal precept in Massachusetts that a person possesses a conditional privilege to publish defamatory information in a commercial context if it furthers a legitimate business interest); *Crump v. Beckley Newspapers, Inc.*, 320 S.E.2d 70, 79, 83 n.5 (W.Va. 1984) (Where the communication of private information is in furtherance of the communicator's legitimate interest or where the communication is for the purpose of another's legitimate interests, the communicator is entitled to a qualified privilege.); *see also* *Retailers Commercial Agency, Inc.*, 174 N.E.2d 376 (1961) (holding that a privilege to dispense legitimate information regarding parties to a commercial transaction exists but is abused, and thereby lost, if it is an "unnecessary, unreasonable or excessive publication of ... defamatory matter" (quoting *Galvin v. New York, New Haven & Hartford, R.R. Co.*, 168 N.E.2d 262, 266 (1960))).

¹⁴⁴ Cavico, *supra* note 143 at 1283 & n.81 (collecting cases).

¹⁴⁵ *Id.* at 1283 & n.82 (collecting cases).

¹⁴⁶ *See* RESTATEMENT (SECOND) OF TORTS § 652G (1977) (stating that "the rules on conditional privilege . . . apply to the publication of any matter that is an invasion of privacy"); Cavico, *supra* note 143, at 1282 & n.80 (collecting cases).

¹⁴⁷ *See generally* Holton, *supra* note 139, at §§ 7-8 (collecting cases); PRIVACY IN THE WORKPLACE 117 (David A. Hoffman, ed. Massachusetts Continuing Legal Education 1994).

¹⁴⁸ Holton, *supra* note 139, at § 7; *O'Brien v. Papa Gino's of Am., Inc.*, 780 F.2d 1067, 1072 (1st Cir. 1986); *Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 567 N.E.2d 912, 915-96 (Mass.1991)

Conversely, in appropriate circumstances, the privacy interest of employees may be created or strengthened by representations made by employers in policy statements or employment manuals. *See, e.g.,*

does not exceed the scope of the consent.¹⁴⁹ Waiver likewise provides a complete defense to a claim of privacy invasion where the employee clearly and unequivocally surrenders his or her right to bring an action for invasion of privacy against the employer, such as through a collective bargaining agreement, an employment contract, or an admission that precludes assertion of the right.¹⁵⁰

When the defense of justification is established and the objective reasonableness of the employer's action is proven, the employer prevails because its intrusive activity cannot be deemed offensive to a reasonable person, notwithstanding its intrusion into the solitude or seclusion of its employee.¹⁵¹ The sufficiency of an employer's justification for intruding on an employee's privacy depends on the validity of the rationale for the intrusion and whether the means or methods used were proportionate to the purported justification for the intrusion.¹⁵²

Finally a common defense to invasion of privacy is the argument that the disclosure of information by the employer was required by legal obligation, duty, or public policy.¹⁵³

When asked to resolve disputes over access to personnel records, courts often assume, without analysis, that the records are confidential.¹⁵⁴ At least one court has

Bratt v. Int'l Bus. Mach. Corp., 785 F.2d 352 (1st Cir. 1986 (employer's confidentiality regulations strengthened employee's claimed interest in not having his medical condition discussed with his supervisor, even by physician engaged by employer to whom supervisor had referred the employee as a result of work-related circumstances); Rulon-Miller v. Int'l Bus. Mach. Corp., 208 Cal. Rptr. 524 (Cal. Ct. App. 1984) (where employer had a stated policy of not interfering with an employee's private life, with certain stated exceptions, the policy gave employees a legitimate expectation of privacy in their personal relationships, which was violated when an employee was confronted and then fired for dating an employee of competitor); O'Connor v. Ortega, 480 U.S. 709 (1987) (public employee had "reasonable expectation" of privacy in the desk and file cabinets in his private office as a result of the employer's policies and practices).

¹⁴⁹ *Id.* An employee's consent to one form of intrusion cannot be extended to entirely different matters by implication. *Id.*; see *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 581 (11th Cir. 1983); *O'Brien*, 780 F.2d at 1072 (holding that consent upon accepting employment to one form of intrusion does not provide blanket consent to other forms of intrusion, even those directed at uncovering the same type of infraction).

¹⁵⁰ *Holton*, *supra* note 139, at § 7.

¹⁵¹ *Id.*

¹⁵² *Id.* at § 8 (collecting cases).

¹⁵³ PRIVACY IN THE WORKPLACE 117 (Massachusetts Continuing Legal Education 1994); see, e.g., *Davis v. Monsanto*, 627 F. Supp. 418 (S.D. W.Va. 1986) (limited disclosure by employer-provided counseling service to employer that employee was suicidal and homicidal was privileged because the disclosure was required by law mandating that employers make workplace safe); *Wells v. Premier Indus. Corp.*, 691 P.2d 765 (Colo. Ct. App. 1984) (employer did not violate an employee's right to privacy where, after notifying employee of its intention to comply with I.R.S. summons, the employer produced the employee's records); *Atchison, Topeka, & Santa Fe Ry. Co. v. Lopez*, 531 P.2d 455 (Kan. 1975) (compliance with a Railway Commission subpoena requiring production of arrest and conviction records of all employees was deemed not to be an invasion of privacy); but see *Saldana v. Kelsey-Hayes Co.*, 443 N.W.2d 382 (Mich. Ct. App. 1988) (holding that employee privacy invasion action could go to jury on question of whether means employer undertook to investigate employee disability claim were justified).

¹⁵⁴ See, e.g., *Frank v. Capital Cities Communications, Inc.*, No. 80 Civ. 2188, 1987 U.S. Dist. LEXIS 9325 (S.D.N.Y. Oct. 14, 1987).

observed that an employee “has little or no privacy interest in her work files, given that such information is the property of her employer.”¹⁵⁵ The cases generally turn on the balancing of interests.

One Massachusetts court rejected a privacy claim arising out of an employer’s disclosure of personnel file information.¹⁵⁶ The employee alleged that her privacy was violated by the following actions:

- The employer disclosed the employee’s salary to her staff assistant,
- The employer disclosed the employee’s thesis proposal to dean at the university,
- The employer disclosed the employee’s job description, and
- Someone intercepted her work papers and computer files while she was out on sick leave.

The court ruled that the employee’s salary, thesis proposal, and job description were not of a “highly personal or intimate nature” and that the disclosures were reasonably related to the employer’s legitimate interest of evaluating the employer’s fitness for her job and her graduate program.¹⁵⁷ The court noted that the employee “has little or no privacy interest in her work files, given that such information is the property of her employer.”¹⁵⁸ Accordingly, the court dismissed the invasion of privacy claim.¹⁵⁹

When an employer reasonably suspects an employee of wrongdoing, the employee’s reasonable expectation of privacy in his or her work records is diminished and is outweighed by the employer’s legitimate interest in furnishing such records to its fidelity insurer in support of a claim.¹⁶⁰ Disclosure of personnel records of a suspected defalcator to a fidelity insurer is justified by legitimate business interests and should not

¹⁵⁵ *Battenfield v. Harvard Univ.*, No. 91-5089-F, 1993 Mass. Super. Lexis 253, at *26 (Aug. 31, 1993).

¹⁵⁶ *Id.* at *25-28. Specifically, the claim was for public disclosure of private facts, pursuant to Massachusetts General Laws Chapter 214, Section 1B, which proscribes disclosure of facts about an individual that are of a highly personal or intimate nature where there exists no legitimate countervailing interests. *Id.* at *25-26 (quotation omitted).

¹⁵⁷ *Id.* *26. Compare *Mulgrew v. Taunton*, 574 N.E.2d 389 (Mass. 1991) (no invasion of privacy when police chief disclosed, in response to city council inquiry, that plaintiff officer performed poorly, abused “sick days,” and left the department in a “cloud of suspicion”); *Hastings & Sons Publ’g Co. v. City Treasurer of Lynn*, 375 N.E.2d 299 (1978) (disclosure of police payroll records did not violate 1B) *with* *Tower v. Hirschhorn*, 492 N.E.2d 728 (1986) (doctor violated 1B by divulging confidential medical information); *Bratt v. Int’l Bus. Mach. Corp.*, 467 N.E.2d 126 (Mass. 1984) (intra-corporate disclosure of plaintiff’s medical diagnosis that he was paranoid could constitute a violation of 1B).

¹⁵⁸ *Battenfield*, at *26.

¹⁵⁹ *Id.* at *27.

¹⁶⁰ See *Nadal-Ginard v. Children’s Hosp. Corp.*, No. 94-3782-E, 1995 Mass. Super. LEXIS 383 (Dec. 1, 1995), *citing* *Conway v. Smerling*, 635 N.E.2d 268 (Mass. App. Ct. 1994), for the proposition that when an employer has a reasonable suspicion that an employee is guilty of embezzlement, the employer is justified in disclosing facts related to the embezzlement.

give rise to liability for invasion of privacy. Such a disclosure also should be protected by the qualified privilege to disclose personal information concerning an employee where reasonably necessary to serve legitimate business interests of the employer.¹⁶¹

In addition, the insured has a contractual duty to cooperate with the investigation and to furnish documents reasonably requested by the fidelity insurer. This duty to cooperate creates a legal obligation to produce the documents that, arguably, should supply a defense to a claim for invasion of privacy.¹⁶²

Care should be taken by the fidelity insurer to limit access to such personnel records to those with a need to know. The insured's concerns about its employee's privacy can be addressed by a confidentiality agreement that appropriately limits use of the records. Finally, the insurer should be clear that it is not seeking any medical information, which is irrelevant to the claim and is subject to an array of statutory safeguards.¹⁶³

5. Retaliatory Litigation

Fidelity professionals long have recognized the possibility that an employee accused of wrongdoing may bring retaliatory litigation against persons who disseminate disparaging information contained in a fidelity proof of loss.¹⁶⁴ One potential claim is for false light invasion of privacy,¹⁶⁵ which imposes liability for publicizing a matter in a manner that casts another in a false light, provided that the false light would be highly offensive to a reasonable person, and that the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.¹⁶⁶ Such a claim might be asserted against a fidelity investigator who allows co-workers and other knowledgeable individuals to review and comment upon allegations in a proof of loss. Will such limited dissemination of the proof of loss subject the investigator to liability for false light invasion of privacy?

A fidelity investigator should not be held liable for false light invasion of privacy provided that he or she has narrowly disseminated a proof of loss to a limited number of persons who possess information relevant to the allegations in the proof of loss.¹⁶⁷ First,

¹⁶¹ RESTATEMENT (SECOND) OF TORTS § 652G, at 401 (1977).

¹⁶² See *infra* note 153, and cases cited therein.

¹⁶³ A discussion of the confidentiality of medical records under HIPAA is beyond the scope of this article.

¹⁶⁴ See, e.g., Keeley & Duffy, *supra* note 1, at 193-96; Harvey C. Koch, *Retaliatory Litigation*, in HANDLING FIDELITY BOND CLAIMS, at 483-502 (Michael Keeley & Timothy M. Sukel, eds. 1999); see also *id.* at 503-04 (appendix of secondary sources concerning fidelity insurance retaliatory litigation).

¹⁶⁵ The risk of liability for defamation has been ably addressed by prior commentators and is beyond the scope of this article. See *infra* note 163.

¹⁶⁶ RESTATEMENT (SECOND) OF TORTS § 652E (1977).

¹⁶⁷ It bears note that "false light" tends to fare poorly, even in those jurisdictions that recognize the tort. McCoy, *supra* note 22, at 449, n.18, and cases cited.

such a claim will fail unless the plaintiff employee satisfies his or her burden of proof to establish that the allegations are false.¹⁶⁸

Second, limited distribution of a proof of loss fails to satisfy the “publicity” element of false light, which requires that the matter be made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge.¹⁶⁹ The “publicity” element is not satisfied by the communication of a fact to a single person or even to a small group of persons.¹⁷⁰

Third, a conditional privilege can shield the publication of private material against liability unless the privilege is abused.¹⁷¹ Publication of private material, such as may be contained in a proof of loss, will be conditionally privileged if the circumstances induce a correct or reasonable belief that there is information that affects a sufficiently important interest of the publisher, and the recipient’s knowledge of the matter will be of service in the lawful protection of the interest.¹⁷²

When a fidelity claim investigator shares a proof of loss with a limited circle of people with knowledge of the transactions at issue, such disclosure should be conditionally privileged. The insurer has a legitimate interest in investigating the insured’s allegations, and advising witnesses of the allegations and obtaining their comment thereon is likely to aid the investigation. The insurer should make sure that the insured has sworn to the contents of the proof of loss, to establish that the insured has a good faith belief in its claim.¹⁷³ The investigator should be careful to share only that information that is necessary to its reasonable investigation of the claim.¹⁷⁴ Deciding which portions of a proof of loss should be shared must be decided on a case-by-case basis after weighing the need for disclosure against the potential harm that would result by doing so.¹⁷⁵

¹⁶⁸ Unlike defamation, truth is not an affirmative defense to a false-light claim; rather, “falsity” is an element of the plaintiff’s claim, on which the plaintiff bears the burden of proof. *Regions Bank v. Plott*, No. 1030436, 2004 Ala. LEXIS 163 (Ala. June 25, 2004) (“falsity is the sine qua non of a false-light claim.”). *Id.* at *10.

¹⁶⁹ RESTATEMENT (SECOND) OF TORTS § 652E cmt. a, *citing* § 652D cmt. a (1977).

¹⁷⁰ *Id.* § 652E cmt. a, *citing* § 652D cmt. a (1977). On the other hand, any publication in a newspaper or a magazine, even of small circulation, or in a handbill distributed to a large number of persons, or any broadcast over the radio, or statement made in an address to a large audience, is sufficient to give publicity within the meaning of the term as it is used in this Section.

¹⁷¹ *Id.* § 652G, at 401 (1977) (providing that the rules on conditional privileges to publish defamatory matter stated in §§ 594 to 598A, and on the special privileges stated in §§ 611 and 612, apply to the publication of any matter that is an invasion of privacy).

¹⁷² *Id.* § 652G, at 401 & § 594, at 263 (1977) (affording the same qualified privilege available to defendants in defamation cases); *see also id.* § 595, at 268 (conditional privilege to publish information for protection of interest of recipient or third person) and *id.* § 596, at 274 (conditional privilege to publish information based on common interest).

¹⁷³ *See Keeley & Duffy, supra* note 1, at 195-96.

¹⁷⁴ *Id.*

¹⁷⁵ *Id.*

IV. Federal Privacy Protection Statutes

A. OVERVIEW

At the federal level, various statutes exist that protect privacy rights. These statutes include (1) the Gramm-Leach-Bliley Act (regulating the collection and distribution of personal and financial information by “financial institutions” including banks and insurance companies);¹⁷⁶ (2) the Electronic Communications Privacy Act (prohibiting unauthorized access to computers);¹⁷⁷ and, (3) the Wiretap Act (prohibiting the interception of data as well as knowing disclosures of such illegally obtained data).¹⁷⁸

¹⁷⁹

B. GRAMM-LEACH-BLILEY ACT¹⁸⁰

1. Introduction

In 1999, Congress passed the Gramm-Leach-Bliley Act¹⁸¹ “to enhance competition in the financial services industry . . . by eliminating many federal and state law barriers to affiliations among banks and securities firms, insurance companies, and other financial service providers.”¹⁸² The GLBA fosters efficiency by facilitating mergers among financial firms.¹⁸³ It enables one-stop shopping for financial services and allows financial supermarkets to share information among affiliates.¹⁸⁴

Recognizing that the adoption of the GLBA would afford financial institutions greater access to customers’ personal financial information, Congress included provisions

¹⁷⁶ 15 U.S.C. §§ 6801-6809 (2004) [hereinafter known as GLBA]. The Gramm-Leach Bliley Act restricts the release by financial institutions of “non-public personal information” to third parties unaffiliated with the financial institution. “Nonpublic personal information:” is defined as “personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution.” *Id.* at § 6809.

¹⁷⁷ 18 U.S.C. §§ 2701-2711 (2004) [hereinafter ECPA]. The statute grants a private civil right of action against violators. *Id.* at § 2707.

¹⁷⁸ 18 U.S.C. §§ 2510-2522 (2004). Like the ECPA, the Wiretap Act also authorizes a private civil right of action. *Id.* at § 2520.

¹⁷⁹ A discussion of state statutory and common law regarding a bank’s obligation to maintain the confidentiality of customer records is beyond the scope of this article. For a compilation of such authorities, see Smith, *supra* note 33 (compiling state statutes on the confidentiality of bank and financial records) and Raymond, *supra* note 123 (collecting and analyzing federal and state cases that discuss whether, and under what circumstances, a bank may be held liable under state law for disclosing financial information concerning a depositor or loan customer).

¹⁸⁰ 15 U.S.C. §§ 80b-6827.

¹⁸¹ The GLBA is also known as the Financial Services Modernization Act of 1999.

¹⁸² *Trans Union LLC v. FTC*, 295 F.3d 42, 46-47 (D.C. Cir. 2002) (quoting from legislative history) (citation omitted), *aff’g*, *Individual Reference Servs. Group Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 18-20 (D.D.C. 2001) (discussing legislative history of the GLBA); *see generally* Jolina C. Cuaresma, *The Graham-Leach-Bliley Act*, 17 BERKELEY TECH. L.J. 497, 498-502 (2002).

¹⁸³ Cuaresma, *supra* note 182, at 501-02.

¹⁸⁴ *Id.*

designed to protect the privacy of “nonpublic personal information”¹⁸⁵ that consumers provide to financial institutions.¹⁸⁶ Title V of the GLBA¹⁸⁷ contains a number of privacy provisions and reflects “the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.”¹⁸⁸ These provisions represent the first piece of federal legislation to establish a minimum federal standard of privacy for financial information.^{189 190}

2. Restriction on Disclosing Non-public Information to Non-Affiliates

The GLBA regulates the sharing of NPI by financial institutions with affiliates¹⁹¹ and non-affiliated third parties.¹⁹² With regard to affiliates, the GLBA merely requires that financial institutions provide their customers with notice of their policies and practices regarding the disclosure of NPI.¹⁹³ While the same requirement also applies to non-affiliates,¹⁹⁴ the GLBA further requires that financial institutions give consumers the ability to direct that NPI not be provided to non-affiliates at all.¹⁹⁵ This requirement is called the right to opt-out.

Specifically, the GLBA restricts the ability of a “financial institution”¹⁹⁶ to disclose NPI to a non-affiliated third party by requiring (subject to certain exceptions)

¹⁸⁵ Hereinafter NPI.

¹⁸⁶ *Trans Union LLC*, 295 F.3d at 46; *N.Y. State Bar Ass’n v. FTC*, 276 F. Supp. 2d 110, 111-12 (D.D.C. 2003).

¹⁸⁷ 15 U.S.C. §§ 6801-6827 (2004).

¹⁸⁸ *Id.* at § 6801(a).

¹⁸⁹ Cuaresma, *supra* note 182, at 502; *see also id.* at 502 n.38, noting: “While Congress has passed several laws protecting informational privacy, no federal law has applied to private companies’ use of financial information. *See* Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 (2001) (providing limits to when banks are obligated to release customer information to government agencies); Privacy Act of 1974, 5 U.S.C. § 552(a) (2001) (providing limits on federal agencies’ collection, use, and disclosure of personally identifiable information).”

¹⁹⁰ Section 6807(b) of the GLBA expressly allows states to enact consumer protection statutes providing greater privacy protection.

The California Financial Information Privacy Act, for example, became operative on July 1, 2004, as California Financial Code §§ 4050-4059. In requiring that consumers be given control over the transmittal of personal financial information both between affiliated business institutions and as to non-affiliated third parties, either through “opt-out” provisions in the case of affiliated institutions or express consent for disclosure to non-affiliates, the California Financial Information Privacy Act affords greater privacy protection than the GLBA. *Am. Bankers Ass’n v. Lockyer*, No. CIV. S 04-0778 MCE KJM, 2004 U.S. Dist. LEXIS 12367 at *4 (E.D. Cal. June 30, 2004) (holding that California Financial Information Privacy Act was authorized by the GLBA’s savings clause, 15 U.S.C. § 6807(b), and was not pre-empted by the Fair Credit Reporting Act).

¹⁹¹ “The term ‘affiliate’ means any company that controls, is controlled by, or is under common control with another company.” 18 U.S.C. § 6809(6) (2004); 16 C.F.R. § 313.3(a). For the definition of “control,” *see* 16 C.F.R. § 313.3(g).

¹⁹² *Lockyer*, 2004 U.S. Dist. LEXIS 12367, at *14-15.

¹⁹³ 15 U.S.C. § 6803(a)(1) (2004).

¹⁹⁴ *Id.*

¹⁹⁵ *Id.* at § 6802(b)(1).

¹⁹⁶ “The term ‘financial institution’ means any institution the business of which is engaging in financial activities described in section 1843(k) of Title 12.” *Id.* at § 6809(3); *see also* 12 C.F.R. § 225.28

that the financial institution provide the consumer with notice of the institution's disclosure policies and the opportunity for the consumer to "opt out" of disclosure."¹⁹⁷ Notably, even though Congress explicitly directs each financial institution to "respect the privacy of its customers,"¹⁹⁸ customers cannot opt-out of information sharing among affiliates.¹⁹⁹

Unless a statutory exception applies, a consumer opt-out would prohibit a bank from disclosing that customer's NPI to a financial institution bond insurer in furtherance of a claim. To understand the limits that the GLBA imposes on investigations involving financial institutions, the following sections examine (1) what is deemed NPI; and (2) what exceptions allow disclosure of NPI when a consumer opts-out.

3. Non-Public Financial Information

The GLBA defines NPI as "personally identifiable financial information--(i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution."²⁰⁰

The GLBA does not define "personally identifiable financial information" ("PIFI"),²⁰¹ but the FTC regulations define the term to mean:

any information:

(i) A consumer provides to you [the regulated financial institution] to obtain a financial product or service from you;

(ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or

(iii) You otherwise obtain about a consumer in connection with providing a financial service product or service to that consumer.²⁰²

Under this definition, PIFI includes information "that may not be considered intrinsically financial."²⁰³ Examples of PIFI include a customer's name, address,

(list of permissible non-banking activities). Financial institutions include businesses that are engaged in banking, insuring, stocks and bonds, financial advice, and investing. It is unlikely that GLBA extends to law firms or lawyers. *See* N.Y. State Bar Ass'n v. FTC, 276 F. Supp. 2d at 128.

¹⁹⁷ 15 U.S.C. §§ 6802(a), (b), (e), 6803 (2004).

¹⁹⁸ *Id.* at § 6801(a).

¹⁹⁹ Cuaresma, *supra* note 182, at 512.

²⁰⁰ 15 U.S.C. § 6809(4)(A) (2004). The FTC regulations also define NFI as PIFI. *See* 16 C.F.R. § 313.3(n)(1).

²⁰¹ *Trans Union LLC v. FTC*, 295 F.3d 42, 49 (D.C. Cir. 2002).

²⁰² 16 C.F.R. § 313.3(o)(1) (F.T.C. Final Rules); *see* Individual Reference Servs. Group Inc. v. F.T.C., 145 F. Supp. 2d 6, 26 (D.D.C. 2001). While this article discusses only the F.T.C. Final Rules, each of the other agencies promulgated an analogous set of regulations. *Id.* at 21 n.10, *citing* OCC Final Rules, 12 C.F.R. § 40.1 *et seq.*, Board Final Rules, 12 C.F.R. § 2216.1 *et seq.*, FDIC Final Rules, 12 C.F.R. § 332.1 *et seq.*, OTS Final Rules, 12 C.F.R. § 573.1 *et seq.*, NCUA Final Rules, 12 C.F.R. § 716.1 *et seq.*

telephone number, mother's maiden name and social security number.²⁰⁴ The regulation provides numerous examples of what constitutes PIFI²⁰⁵ and what doesn't.^{206 207}

The expansive definition of PIFI encompasses materials that traditionally are requested in the investigation of financial institution bond claims. For instance, loan files requested in a loan loss case would be replete with PIFI. Thus, financial institution bond claim investigations may be hampered unless the circumstances fit one of the GLBA's express exceptions to the prohibition on disclosing PIFI to non-affiliate third parties where a customer has opted-out.

4. Exceptions

There are a series of exceptions under GLBA that permit information sharing with non-affiliate third parties even where the customer has opted-out.²⁰⁸ Several of these exceptions are pertinent to the issue of whether a bank may disclose non-public personal information to a fidelity insurer in support of a bond claim.

Notably, information may be disclosed "with the consent or at the direction of the consumer."²⁰⁹ In the event that a customer suffers a loss in their account in connection

²⁰³ *Individual Reference Servs. Group Inc.*, 145 F. Supp. 2d at 21.

²⁰⁴ *Id.* at 40 (rejecting challenge by credit reporting agency that regulation's definition of the statutory term "personally identifiable financial information" was overbroad, inconsistent with the GLBA, and violative of constitutional rights).

²⁰⁵ The regulation provides the following examples of PIFI:

(A) Information a consumer provides to [a regulated financial institution] on an application to obtain a loan, credit card, or other financial product or service;

(B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;

(C) The fact that an individual is or has been one of [a regulated financial institution's] customers or has obtained a financial product or service from [a regulated financial institution];

(D) Any information about [a regulated financial institution's] consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;

(E) Any information that a consumer provides to [a regulated financial institution] or that [a regulated financial institution] or [its] agent otherwise obtain in connection with collecting on, or servicing, a credit account;

(F) Any information [a regulated financial institution] collect[s] through an Internet "cookie" (an information collecting device from a web server); and

(G) Information from a consumer report.

116 C.F.R. § 313.3(o)(2)(i).

²⁰⁶ The regulation expressly excludes the following from the definition of PIFI:

(A) A list of names and addresses of customers of an entity that is not a financial institution; and

(B) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

116 C.F.R. § 313.3(o)(2)(ii).

²⁰⁷ To date industry challenges to these expansive regulations have failed. See, e.g., *Individual Reference Servs. Group Inc.*, 145 F. Supp. 2d at 40.

²⁰⁸ 15 U.S.C. § 6802(e)(1)-(8) (2004).

²⁰⁹ *Id.* at § 6802(e)(2).

with a fidelity claim, one would expect the customer to consent to disclosure of his or her account records to the insurer. Of course, if the customer is in conspiracy with the defalcating employee, consent may be withheld.

None of the other exceptions expressly authorizes disclosure in connection with a fidelity bond investigation. However, several other exceptions might apply. Arguably disclosure of PFI in support of a fidelity bond claim is a component of “required institutional risk control” and may assist in “resolving customer disputes or inquiries.”²¹⁰ Seeking indemnity of fraud losses under a fidelity bond arguably serves to “protect against ... actual or potential fraud, unauthorized transactions, [or] claims ...”²¹¹ Definitive evaluation of the applicability of the exceptions is hampered because these terms are undefined by statute or regulation and have yet to be interpreted by case law.²¹²

C. FEDERAL WIRETAPPING STATUTES

In addition to state common law privacy claims, an employee whose e-mail, phone calls or voicemail have been accessed may assert claims under federal wiretapping statutes.²¹³ Such federal claims may arise in the context of a fidelity bond claim. There

²¹⁰ *Id.* at § 6802(e)(3)(C) (allowing disclosure “for required institutional risk control, or for resolving customer disputes or inquiries”).

²¹¹ *Id.* at § 6802(e)(3)(B) (allowing disclosure “to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability”).

²¹² Several other exceptions should also be considered. Disclosure is permitted:

(4) to provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the financial institution, persons assessing the institution’s compliance with industry standards, and the institution’s attorneys, accountants, and auditors;

(5) to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, . . . to law enforcement agencies, . . . self-regulatory organizations, or for an investigation on a matter related to public safety;

....

(8) to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.

Id. at § 6802(e)(4), (5), (8).

²¹³ State wiretapping statutes are beyond the scope of this article. For a survey of state wiretapping laws, see Andrew Charlesworth, *Information Privacy Law in the European Union: E Pluribus Unum or Ex Uno Plures?*, 54 HASTINGS L. J. 931, 987-1162 (2003) (Appendix A: State Wiretap Laws as of June 1, 2002).

One commentator offers the following catalogue of federal and state sources of privacy protection for employee’s aggrieved by employer workplace monitoring:

Title III and the ECPA are by no means the only source of redress for an employee aggrieved by employer workplace monitoring. In addition to other federal enactments protecting privacy, such as the Communications Act of 1934, 47 U.S.C. § 605 (1988), and FCC regulations, 47 C.F.R. § 2.701 (1993), and common law tort claims for invasion of privacy, the following state legislatures have created their own private rights of action for illegal wiretapping, which substantially parallel federal law. Most of these states award actual or statutory damages of \$100 per day of violation or \$1000, whichever is greater, in addition to reasonable attorney’s fees and costs. *See* CAL. PENAL CODE § 629.36 (West Supp. 1994) (establishing civil remedies for any person whose wire or oral

communication is intercepted, including actual damages, “but not less than liquidated damages” of \$100 per day for each day violation continued or \$1000, whichever is greater, punitive damages, reasonable attorney’s fees, and other costs of litigation); DEL. CODE ANN. tit. 11, § 1336(w) (1987) (establishing civil remedy for any person whose wire or oral communications are intercepted and allowing for recovery of either actual damages or statutory damages of \$100 per day for each day violation continued or \$1000, whichever is greater, punitive damages, attorney’s fees, and litigation costs); D.C. CODE ANN. § 23-554(a) (1981) (providing civil remedies for any person whose wire or oral communications are intercepted, including actual damages or greater of liquidated damages of \$100 per day for each day of violation or \$1000, punitive damages, reasonable attorney’s fees, and costs); FLA. STAT. ch. 934.10 (1993) (establishing private right of action for any person whose wire or oral communication is intercepted and allowing for recovery of actual damages or statutory damages of either \$100 per day for each day violation continued, or \$1000, whichever is greater, punitive damages, reasonable attorney’s fees, and costs); HAW. REV. STAT. § 803-48(A)-(C) (1985 & Supp. 1992) (providing civil remedy for any person whose wire, oral, or electronic communications are accessed or intercepted and allowing for recovery of actual damages or greater of liquidated damages of \$100 per day for each day of violation or \$10,000, punitive damages, reasonable attorney’s fees, and court costs, or equitable or declaratory relief where appropriate); IDAHO CODE § 18-6709 (Michie 1987) (creating private right of action for any person whose wire or oral communications are intercepted and allowing for recovery of either actual damages or statutory damages of \$100 per day for each day of violation or \$1000, whichever is greater, punitive damages, reasonable attorney’s fees, and litigation costs); 720 ILL. COMP. STATE ANN. 5/14-6(1) (West 1993) (providing for civil remedies where eavesdropping on conversation has occurred, and allowing for injunction against further eavesdropping, and actual and punitive damages); IND. CODE § 35-33.5-5-4(a) (1993) (establishing private right of action for any person whose communications are intercepted, and providing for recovery of either actual damages, but not less than liquidated damages of \$100 per day for each day of violation or \$1000, whichever is greater, punitive damages, reasonable attorney’s fees, and court costs); IOWA CODE ANN. § 808B.8.1 (West 1994) (extended to July 1, 1999) (allowing any party whose wire or oral communications are intercepted to recover greater of actual damages or statutory damages of not less than \$100 per day for each day of violation or \$1000, punitive damages, attorney’s fees, and costs); KAN. STAT. ANN. § 22-2518(1) (1988) (establishing private right of action for any person whose wire, oral, or electronic communications are intercepted, and allowing for recovery of actual damages or statutory damages of either \$100 per day for each day violation continued or \$1000, whichever is greater, punitive damages, reasonable attorney’s fees, and costs); ME. REV. STAT. ANN. tit. 15, § 711 (West 1980 & Supp. 1993) (creating civil remedy for any person whose conversation is intercepted in violation of this section, and providing for recovery of actual damages, but not less than liquidated damages of \$100 per day for each day of violation, attorney’s fees, and costs); MD. CODE ANN., CTS. & JUD. PROC. § 10-410(a) (1993) (providing civil remedy for any person whose wire, oral, or electronic communications are intercepted and allowing recovery of either actual damages, or greater of statutory damages of \$100 per day for each day violation continued, or \$1000, punitive damages, attorney’s fees, and costs); MASS. GEN. LAWS ANN. ch. 272, § 99Q (West 1990) (establishing civil remedy for any person whose wire or oral communications are intercepted, and providing for recovery of either actual damages or statutory damages of \$100 per day for each day violation continued, or \$1000, whichever is greater, punitive damages, attorney’s fees, and costs); MICH. COMP. LAWS ANN. § 750.539h (West 1991) (allowing any party on whom eavesdropping is practiced to receive an injunction, and actual and punitive damages); MINN. STAT. ANN. § 626A.13(1)-(3) (West 1983 & Supp. 1994) (providing civil remedy for any person whose wire, electronic, or oral communication is intercepted, and allowing for temporary or other equitable or declaratory relief, treble damages or statutory damages of \$100 per day

for each day of violation or \$10,000, whichever is greater, attorney's fees, and litigation costs); MISS. CODE ANN. § 41-29-529(1) (1993) (establishing civil remedy for any person whose wire or oral communications are intercepted and allowing for recovery of actual damages or statutory damages of \$100 per day for each day violation continued or \$1000, whichever is greater, punitive damages, attorney's fees, and costs); NEB. REV. STAT. § 86-707.02 (Supp. 1992) (creating private right of action for any person whose wire, oral, or electronic communications are intercepted, and providing for preliminary or equitable or declaratory relief, actual damages or greater of statutory damages of \$100 per day for each day of violation or \$10,000, and attorney's fees); N.H. REV. STAT. ANN. § 570-A:11 (1986) (providing civil action to any person whose wire or oral communications are intercepted and allowing recovery of actual damages or greater of statutory damages of \$100 per day for each day violation continued or \$1000, punitive damages, attorney's fees, and costs); N.J. STAT. ANN. § 2A:156A-24(a)-(c) (West 1985 & Supp. 1994) (extended to July 1, 1999) (establishing private right of action for any person whose wire or oral communications are intercepted and allowing recovery of actual damages or greater of statutory damages of \$100 per day for each day violation continued or \$1000, punitive damages, attorney's fees, and costs); N.M. STAT. ANN. § 30-12-11(A) (Michie 1984) (establishing private right of action for any person whose wire or oral communications are intercepted and allowing recovery of actual damages or greater of statutory damages of \$100 per day for each day violation continued or \$1000, punitive damages, attorney's fees, and costs); OHIO REV. CODE ANN. § 2933.65(A) (West 1992) (establishing private right of action for any person whose wire or oral communications are intercepted and allowing recovery of actual damages or \$200 per day for each day violation continued up to \$2000, punitive damages, attorney's fees, and costs); OR. REV. STAT. § 133.739(1) (1993) (providing civil cause of action to any person whose wire, oral, or electronic communications are intercepted and allowing recovery of actual damages, but not less than \$100 per day for each day violation continued or \$1000, whichever is greater, punitive damages, and attorney's fees at trial and on appeal); PA. CONS. STAT. ANN. § 5725(a) (West 1983 & Supp. 1992) (creating private right of action for any person whose wire, oral, or electronic communications are intercepted and allowing for recovery of actual damages or greater of statutory damages of \$100 per day for each day of violation or \$1000, punitive damages, attorney's fees, and costs); R.I. GEN. LAWS § 12-5.1-13 (1981) (establishing civil remedy for any person whose wire or oral communications are intercepted and allowing recovery of actual damages or greater of statutory damages of \$100 per day for each day violation continued or \$1000, punitive damages, attorney's fees, and litigation costs); UTAH CODE ANN. § 77-23a-11(1)-(3) (1990) (providing private right of action for any person whose wire, oral, or electronic communications are intercepted and allowing for preliminary or other equitable or declaratory relief as appropriate or statutory damages of \$100 per day for each day of violation or \$10,000, whichever is greater, punitive damages and, attorney's fees, and costs); VA. CODE ANN. § 19.2-69 (Michie 1990) (establishing civil cause of action for any person whose wire, oral, or electronic communications are intercepted and allowing for recovery of actual damages or greater of statutory damages of \$100 per day for each day violation continued or \$1000, punitive damages, attorney's fees, and costs); WASH. REV. CODE § 9.73.060 (1992) (providing private right of action for any person whose privacy is violated within meaning of this chapter and allowing recovery of actual damages, including mental pain and suffering, or statutory damages of \$100 per day for each day of violation up to \$1000, attorneys fees, and costs); W. VA. CODE ANN. § 62-1D-12(a) (Michie 1992) (establishing civil remedy for any person whose wire, oral, or electronic communications are intercepted and allowing for recovery of actual damages, but not less than \$100 per day for each day violation continued, punitive damages, attorney's fees, and costs); WIS. STAT. ANN. § 968.31(2m) (West Supp. 1993) (providing civil remedy for any person whose wire, oral, or electronic communications are intercepted and allowing recovery of actual damages or greater of statutory damages of \$100 per day for each day violation continued or \$1000, punitive damages, attorney's

may be circumstances in which an insured monitors telephone calls or reviews e-mails of an allegedly dishonest employee to determine whether a bond claim exists, or to gather documentation in support of a claim. The employer may review e-mails on the employee's hard drive or company back-up tapes. Perhaps a supervisor will secretly listen to workplace telephone conversations involving the employee. An employee may listen to a colleague's voicemail message, inadvertently or otherwise, and discover evidence that the colleague has acted dishonestly.²¹⁴

In the event that such monitoring yields evidence of employee dishonesty, the insured likely would submit the information in support of its fidelity bond claim. It is not unusual for an employer to provide its fidelity insurer with copies of e-mails to or from the principal to substantiate a fidelity claim. Where relevant, information gleaned from monitoring telephone calls or listening to voicemails might also be submitted to the insurer. These situations raise the question of whether such access to workplace communications violates federal wiretapping statutes. When such materials are submitted in connection with a fidelity claim investigation, does the insurer face liability under wiretapping statutes?

a. Overview

In 1986, Congress passed the Electronic Communications Privacy Act²¹⁵ in order to ensure the security of electronic communications.²¹⁶ In Title I, the ECPA amended the

fees, and costs); WYO. STAT. ANN. § 7-3-609(a) (Michie 1987 & Supp. 1993) (creating private right of action for any person whose wire, oral, or electronic communications are intercepted and allowing recovery of actual damages, but not less than \$1000 per day for each day violation continued, punitive damages, attorney's fees, and costs).

Further, many states recognize both common law and statutory rights to privacy, which can be used as the basis for civil damages against invasions of privacy. See Privacy for Consumers and Workers Act: Hearing on S.984 Before the Subcomm. on Employment and Productivity of the Senate Comm. on Labor & Human Resources, 101st Cong., 1st Sess. 23-24 (1993) (Statement of Lewis L. Maltby, Director, ACLU National Task Force on Civil Liberties in the Workplace) (noting that almost all states have common law right to privacy, but recognizing limitation of common law in employment context). This Comment, however, focuses only on the private rights of action created under Title III and the ECPA.

Thomas R. Greenberg, *Comment, E-Mail and Voice Mail: Employee Privacy and The Federal Wiretap Statute*, 44 AM. U.L. REV. 219, 223 n.16 (1994).

²¹⁴ As noted by one commentator: "[G]rowing reliance by businesses on E-mail and voice mail communications systems has created many new opportunities for private sector employers to monitor the performance and conduct of their employees without the employees knowing." *Id.* 221-22 and nn.7-10 (discussing survey of employers in a "broad spectrum of industries" showing that twenty-two percent of the respondents had "engaged in searches of employee computer files, voice mail, electronic mail, or other networking communications." Of that twenty-two percent of employers, slightly more than sixty-six percent of them confirmed that they conducted employee monitoring without the employees' knowledge or consent.").

²¹⁵ 18 U.S.C. §§ 1367-3127 (2004) [hereinafter ECPA].

²¹⁶ *Quon v. Arch Wireless Operating Co.*, 309 F. Supp. 2d 1204, 1207 (C.D. Cal. 2004). "Title I of the ECPA amended the federal Wiretap Act, which previously addressed only wire and oral communications, to "address[]the interception of . . . electronic communications." *Konop v. Hawaiian*

Wiretap Act,²¹⁷ and in Title II it created the Stored Communications Act.²¹⁸ Congress enacted the ECPA “to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.”²¹⁹

The ECPA is the primary federal legal protection against the unauthorized interception, accessing, use or disclosure of electronic communications while in transit or in storage. The ECPA prohibits both illegal interceptions of electronic communications²²⁰ and illegal access to stored electronic communications.²²¹

The Wiretap Act has been characterized as “famous (if not infamous) for its lack of clarity.”²²² The intersection of the Wiretap Act and the Stored Communications Act “is a complex, often convoluted, area of law.”²²³ The difficulty is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web.²²⁴ As a result, the existing statutory framework is ill-suited to address modern forms of communication.²²⁵

2. Substantive Provisions of Title I of the ECPA

Title I of the ECPA prohibits:

- the intentional interception of wire, oral, or electronic communications,²²⁶
- the intentional disclosure of the contents of a wire, oral, or electronic communication by one knowing or having reason to know that the

Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002), *quoting* S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3557.

²¹⁷ For an overview of the Wiretap Act of 1968, formally known as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, see Greenberg, *supra* note 212, at 225-32.

²¹⁸ *Quon*, 309 F. Supp. 2d at 1207.

²¹⁹ *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 633 (E.D. Pa. 2001) (citation omitted), *aff'd in pertinent part*, *Richard Fraser A/B v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3d Cir. 2003); *see also* *Theofel v. Farey-Jones*, 341 F.3d 978, 982 (9th Cir. 2003) (noting that the “[Stored Communications] Act reflects Congress’s judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility”); S. Rep. No. 541, 99th Cong., 2d Sess. 1-2, reprinted in 1986 U.S.C.C.A.N. 3555, 3555-56, *quoted in* Greenberg, *supra* note 212, at 224 n.17 (“The ECPA was intended to ‘update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies,’ and to offset the fact that the existing Title III was ‘hopelessly out of date.’”). *Id.* at 232.

²²⁰ 18 U.S.C. §§ 2510-2522 (2004).

²²¹ *Id.* at § 2701-2711. The 1986 amendments, Pub. L. 99-508, 100 Stat. 1848 (1986), extended the coverage of Title III to electronic communications, cellular telephones, and data transmissions, added or altered definitions to correspond with the expanded coverage, added new penalty provisions, increased the range of offenses that can be investigated by a Title III order, and made several procedural changes in the statute. Provisions were also added to regulate the use of pen registers and trace devices, and the acquisition of toll records. Greenberg, *supra* note 212, at n.61.

²²² *Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457, 462 (5th Cir. 1994).

²²³ *United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998).

²²⁴ *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d at 868, 874 (9th Cir. 2002).

²²⁵ *Id.*

²²⁶ 18 U.S.C. § 2511(1)(a) (2004).

information was obtained through an interception that violates the act,²²⁷ and

- the intentional use of the contents of a wire, oral or electronic communication, knowing or having reason to know that information was obtained through the interception of a wire, oral or electronic communication in violation of the statute.²²⁸

a. “Electronic Communication”

The ECPA defines “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce”²²⁹ The definition expressly excludes “any wire or oral communication”²³⁰ Although not specifically referenced in the definition of “electronic communication,” case law establishes that the Wiretap Act applies to “interception” of telephone calls,²³¹ voicemail²³² and e-mail.²³³

b. “Intercept”

Under the Wiretap Act, “intercept” is defined as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.”²³⁴ Standing alone, this definition would seem to suggest that an individual “intercepts” an electronic communication merely by “acquiring” its contents, regardless of when or under what circumstances the acquisition

²²⁷ *Id.* at § 2511(1)(c).

²²⁸ *Id.* at § 2511(1)(d).

²²⁹ *Id.* at § 2510(12).

²³⁰ *Id.* at § 2510(12)(A).

²³¹ *See, e.g.,* *Watkins v. L.M. Berry*, 704 F.2d 577 at 581-82 (denying employer’s summary judgment motion seeking dismissal of federal wiretapping claim based on allegedly unconsented monitoring of employee personal phone calls).

²³² *See, e.g.,* *United States v. Smith*, 155 F.3d 1051 (9th Cir. 1998) (act of retrieving and recording a voicemail message constituted an “interception” and is, therefore, governed by the Wiretap Act).

²³³ *Cf. Wesley College v. Pitts*, 974 F. Supp. 375 (D. Del. 1997), *aff’d*, 172 F.3d 861 (3d Cir. 1998) (Computer programmer could not be liable under ECPA, to extent he inadvertently glimpsed e-mail on computer screen while helping someone, because § 2510(4) defines “intercept” as “acquisition of contents of any wire, electronic, or oral communication through use of any electronic, mechanical, or other device.”); *Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457, 461 (5th Cir. 1994) (Secret Service seizure of a computer containing unread e-mail messages was not an “interception” because of lack of contemporaneity with transmission); *but see* *Greenberg, supra* note 212, at 223-24 and nn.17-19. (“[T]he Wiretap statute has been judicially interpreted to offer a limited degree of privacy protection for the telephone communications of private-company employees. Whether such protection extends to e-mail and voice mail communications is presently unclear, although some commentators have suggested that Title III and the ECPA do not encompass these technologies with respect to private employers.”).

²³⁴ 18 U.S.C. § 2510(4) (2004).

occurs.²³⁵ Courts, however, have clarified that Congress intended a narrower definition of “intercept” with regard to electronic communications.²³⁶

Numerous courts have ruled that an interception must be contemporaneous with transmission for it to fall within the scope of the Wiretap Act.²³⁷ Under this line of authority, electronic communications can only be “intercepted” in violation of Title I when they are in transit, not already in storage.²³⁸

In other words, the act of “interception” cannot occur after an e-mail is received.²³⁹ Applying this principle, a plaintiff has no cognizable claim under the Federal Wiretap Act where the plaintiff’s e-mail was acquired by the former employer from its electronic storage facility after the addressee had received and read it.²⁴⁰

Merely reading an e-mail on the computer screen of the author or recipient does not violate the ECPA.²⁴¹ “This is so because the ECPA defines ‘intercept’ as the ‘acquisition of the contents of any wire, electronic, or oral communication *through the use of any electronic, mechanical, or other device*[,]’²⁴²

Few seizures will constitute interceptions under this narrow reading of the Wiretap Act.²⁴³ The Electronic Communications Privacy Act deliberately is structured to

²³⁵ Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002).

²³⁶ *Id.*

²³⁷ *See, e.g., Steve Jackson Games, Inc.*, 36 F.3d at 461 (Secret Service seizure of a computer containing unread e-mail messages was not an “interception” because of lack of contemporaneity with transmission); *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623 (E.D. Pa. 2001) (disgruntled insurance agent has no viable claim against insurer under Federal Wiretap Act, where it is undisputed that insurer acquired e-mail that agent sent to another agent from its electronic storage facility after other agent had received and read it, because insurer’s retrieval of e-mail message from post-transmission storage, after transmission was complete, was no “interception”), *aff’d in pertinent part*, *Richard Fraser A/B v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3d Cir. 2003); *Eagle Inv. Sys. Corp. v. Tamm*, 146 F. Supp. 2d 105 (D. Mass. 2001) (the Wiretap Act only prohibits the unauthorized interception of electronic communication during transmission; ECPA did not eliminate the during-transmission requirement from the Wiretap Act; granting motion to dismiss claim under Wiretapping Act where defendants acquired an e-mail after it had been sent by plaintiff and received by its intended recipients); *Wesley College*, 974 F. Supp. at 385 (“each court to consider the question has concluded there can be no interception under Title I if the acquisition of the contents of electronic communications is not contemporaneous with their transmissions”) (collecting cases); *see also* *United States v. Turk*, 526 F.2d 654, 658 (5th Cir. 1976) (interpreting 18 U.S.C. § 2511 prior to the 1986 amendments).

²³⁸ *See infra* note 236.

²³⁹ *Garrity v. John Hancock Mut. Life Ins. Co.*, No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002), *citing Eagle*, 146 F. Supp. 2d at 105, and *Steve Jackson Games, Inc.*, 36 F.3d at 462.

²⁴⁰ *Fraser*, 135 F. Supp. 2d at 623, *aff’d in pertinent part*, *Richard Fraser A/B*, 352 F.3d at 107; *Eagle*, 146 F. Supp. 2d at 105.

²⁴¹ *Wesley College*, 974 F. Supp. at 375 (computer programmer could not be liable under ECPA, to extent he inadvertently glimpsed e-mail on computer screen while helping someone).

²⁴² *Id.*, *quoting* 18 U.S.C. § 2510(4) (emphasis added by court) (rejecting plaintiff’s argument that a computer screen can be considered the “electronic device” by which the defendant acquired his information).

²⁴³ *See* *United States v. Steiger*, 318 F.3d 1039, 1047-51 (11th Cir. 2003) (holding intercept did not occur because there was no contemporaneous acquisition but commenting that under the narrow

afford electronic communications in storage less protection than other forms of communication.²⁴⁴

3. Defenses

The SCA provides several statutory exemptions that are significant with respect to liability for interception of the telephone calls and voice messages: the consent and business extension exemptions.

a. Consent Exemption

The ECPA includes an express exemption for interceptions made with the consent of one of the parties to the communication.²⁴⁵ Under the express consent exemption, if one of the parties to an electronic communication consents to another person's interception of the communication, there is no violation of the ECPA unless the interception, at the time it occurred, was committed for a criminal or tortious purpose.²⁴⁶ Consent may be implied or express, but "implied consent should not be casually inferred."²⁴⁷

A consent defense may be raised by an employer who notifies its employees that their phone calls or e-mails are monitored.²⁴⁸ The success of this defense may depend on the scope of the warning. The consent defense has been rejected when an employer merely warned of "limited monitoring."²⁴⁹ Employers have prevailed on a consent

reading of the statute few seizures will constitute interceptions under Wiretap Act); *see also* United States v. Councilman, 373 F.3d 197, 203 (1st Cir. 2004) ("It may well be that the protections of the Wiretap Act have been eviscerated as technology advances.").

²⁴⁴ Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 877 (9th Cir. 2002).

²⁴⁵ 18 U.S.C. § 2511(2)(d) ("It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral or electronic communication . . . where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortuous act . . .").

²⁴⁶ *Id.*

²⁴⁷ "Consent need not be explicit; instead, it can be implied. Implied consent is not, however, constructive consent. Rather, implied consent is consent in fact which is inferred from surrounding circumstances indicating that the party knowingly agreed to the surveillance. In light of the prophylactic purposes of Title III, implied consent should not be casually inferred." Williams v. Poulos, 11 F.3d 271, 281 (1st Cir. 1993) (citations and quotations omitted); *see, e.g.*, Griggs-Ryan v. Smith, 904 F.2d 112, 117 (1st Cir. 1990) (implied consent inferred where defendant was informed (1) that all incoming calls, (2) on a particular line, (3) would be tape recorded).

²⁴⁸ The consent exemption has also been raised in litigation involving the Internet. *See, e.g.*, Konop v. Hawaiian Airlines Inc., 236 F.3d 1035, 1041, 1048 (9th Cir. 2001) (reversing grant of summary judgment in favor of corporate defendant that had accessed the plaintiff's password protected Web site under false pretenses and viewed its contents; holding that "the contents of secure websites are 'electronic communications' in intermediate storage that are protected from unauthorized interception under the Wiretap Act").

²⁴⁹ *See, e.g.*, Watkins v. L.M. Berry, 704 F.2d 577, 581-82 (11th Cir. 1983) (where employee consented to a policy of monitoring sales calls but not personal calls, court rejected defendant employer's summary judgment motion based on consent defense, finding fact questions as to whether interception went beyond point necessary to determine that call was personal) ("knowledge of the *capability* of monitoring alone cannot be considered implied consent").

defense when they made the employee aware of a “strong probability” or “certainty” that calls are monitored.²⁵⁰

b. Business Extension Exemption

The Wiretap Act provides an exemption, known as the “business extension” exception, for interceptions by a telephone “being used by the subscriber or user in the ordinary course of its business.”²⁵¹ Courts have held that if an intercepted call is a business call, then the employer’s monitoring of it is in the ordinary course of business. If it is a personal call, the monitoring is probably, but not certainly, *not* in the ordinary course of business.²⁵² Under the Wiretap Act, an employer is obliged to cease listening as soon as the employer determines that a monitored call is personal, regardless of the contents of the legitimately heard conversation.²⁵³

In the event that an insured offers the contents of intercepted telephone calls or voicemails in support of a fidelity claim, care should be taken to ensure either that the materials relate to business, not personal, matters, or that there was adequate consent to monitoring.

4. Relief

This section of ECPA authorizes injunctions, damages (including punitive damages where appropriate) and attorneys’ fees.²⁵⁴ Prevailing plaintiffs may receive the greater of (a) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violations, or (b) statutory damages of either \$100 a day for each day of violation or \$10,000.00.²⁵⁵

²⁵⁰ See, e.g., *Jandak v. Village of Brookfield*, 520 F. Supp. 815, 824-25 (N.D. Ill. 1981) (police officer whose call was intercepted knew or should have known that the line he was using was constantly taped for police purposes; furthermore, an unmonitored line was provided expressly for personal use); *Simmons v. Southwestern Bell Tel. Co.*, 452 F. Supp. 392, 393-94 (W.D. Okla. 1978) (plaintiff made personal call on telephones which were to be used exclusively for business calls and which were regularly monitored. He had been warned on previous occasions to stop making personal calls from his business telephone; other telephones were specifically provided for personal use), *aff’d*, 611 F.2d 342 (10th Cir. 1979).

²⁵¹ *Watkins*, 704 F.2d at 580-581, *citing* 18 U.S.C. § 2510(5), which provides that “‘electronic, mechanical or other device’ [in § 2511(1)(b)] means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than--(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business.” Furnished, in this case, means a standard extension telephone.

²⁵² *Id.* at 582; *Fischer v. Mt. Olive Lutheran Church*, 207 F. Supp. 2d 914, 922-23 & 926 (W.D. Wis. 2002) (genuine issues of material fact as to whether telephone conversation between youth minister and former tutor, undertaken for an alleged counseling purpose, was business or personal in nature, precluded summary judgment for defendants on minister’s claim against church for ECPA violation).

²⁵³ *Fischer*, 207 F. Supp. 2d at 923, *citing* *Watkins*, 704 F.2d at 584.

²⁵⁴ 18 U.S.C. § 2520(b) (2004).

²⁵⁵ *Id.* at § 2520(c)(2).

5. Electronic Communications Storage Act

The Electronic Communications Storage Act²⁵⁶ was intended to address “access to stored wire and electronic communications and transactional records.”²⁵⁷ Among other things, the SCA defines the conditions in which an electronic communications service may divulge the contents of electronic communications.²⁵⁸ Specifically, the SCA provides that “a person or entity providing electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.”²⁵⁹ The SCA allows for a private right of action for any person aggrieved by any violation of the SCA²⁶⁰ and adopts the same definitions used in the federal Wiretap Act.²⁶¹

a. “Electronic Storage”

“Electronic storage” is defined as “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.”²⁶² Either part of the definition of “electronic storage” is sufficient under the SCA.²⁶³

At least one court has held that the SCA applies to interception of an electronic message only while it is in intermediate storage with the server before being sent to the intended recipient, a window of time which may last a fraction of a second.²⁶⁴ Other courts have held that the SCA is violated by accessing e-mails in storage after receipt by their intended recipient.²⁶⁵ The Stored Communications Act indicates that an email

²⁵⁶ *Id.* at §§ 2701-2711, encompassed as part of the ECPA [hereinafter SCA].

²⁵⁷ *Quon v. Arch Wireless Operating Co. Inc.*, 309 F. Supp. 2d 1204, 1207 (C.D. Cal. 2004), quoting S. Rep. No. 99-541, at 3.

²⁵⁸ *Lopez v. First Union Nat’l Bank*, 129 F.3d 1186, 1189 (11th Cir. 1997), citing 18 U.S.C. § 2702(a)(1).

²⁵⁹ 18 U.S.C. § 2702(a)(1) (2004).

²⁶⁰ *Id.* at § 2707.

²⁶¹ *Id.* at § 2711.

²⁶² 18 U.S.C. §§ 2510(17) and 2711(1) (definitions of Wiretap Act applicable to Stored Communications Act). 18 U.S.C. § 2510(15) defines “electronic communication service” as any service that provides to users thereof the ability to send or receive wire or electronic communications.

²⁶³ *Quon v. Arch Wireless Operating Co.*, 309 F. Supp. 2d at 1207.

²⁶⁴ *See, e.g., Fraser v. Nat’l Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001) (holding that a company’s post-transmission retrieval of the plaintiff’s e-mail messages sent using the company’s electronic messaging server did not violate the SCA; the SCA provides protection only for messages while they are in the course of transmission).

²⁶⁵ *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878-79 (9th Cir. 2002) (court held that, while a defendant’s unauthorized disclosure of the contents of the plaintiff’s secure website did not violate the Wiretap Act, it did violate the SCA. In order for an electronic message to be intercepted under the Wiretap Act, the court said, the electronic message must be acquired during transmission. The SCA, on the other hand, relates to electronic messages that are not intercepted, but rather are extracted from electronic storage.); *Fischer v. Mt. Olive Lutheran Church*, 207 F. Supp. 2d 914, 925 (W.D. Wis. 2002) (the court determined that e-mail was in “electronic storage” for purposes of the SCA when it was retrieved from plaintiff’s e-mail account after transmission).

message is protected while stored at “a facility through which electronic communication service is provided.”²⁶⁶

By way of illustration, where a service provider had a contract with a city to provide an alphanumeric pager service, and the city requested and received from the provider, without a warrant, subpoena or consent of the employees, transcripts of private text messages sent and received by the employees, the employees stated a cognizable claim against the service provider for violation of the Stored Communications Act.²⁶⁷

In *Lopez v. First Union National Bank*, the Eleventh Circuit held that a bank customer stated a cognizable claim under 18 U.S.C. § 2702(a)(1) of the SCA when the defendant bank divulged account information to law enforcement officials pursuant to verbal instructions without a warrant.²⁶⁸ The Court rejected the bank’s argument that the customer failed to state a viable claim because it was not an “electronic communication service.”²⁶⁹ The Court viewed the bank’s argument as “nothing more than deny[ing] the allegations in the plaintiff’s complaint,” which the court was required to accept as true for purposes of the motion to dismiss.²⁷⁰

V. Conclusion

In America, privacy is a cherished value that is protected by a patchwork of laws. A common thread of privacy laws is that an individual’s reasonable expectation of privacy is weighed against legitimate countervailing interests. Employers and their fidelity insurers share a legitimate business interest in resolving fidelity claims based on consideration of all documentation relevant to the circumstances of the claim. Where common sense is employed in the means and manner of gathering and handling personal material, a fidelity investigator should be able to gather documents pertinent to an alleged employee defalcation while respecting recognized rights of privacy.

²⁶⁶ 18 U.S.C. § 2701(a); *see also* United States v. Moriarty, 962 F. Supp. 217 (D. Mass. 1997).

²⁶⁷ *Quon*, 309 F. Supp. 2d at 1204.

²⁶⁸ 129 F.3d 1186, 1189-90 (11th Cir. 1997).

²⁶⁹ *Id.* at 1190.

²⁷⁰ *Id.* at 1189-90.