Chapter Thirteen

Privacy

Phyllis Karasov
Larkin Hoffman
Minneapolis

The author wishes to thank the following individuals for their assistance in the preparation of this chapter: Glenna Gilbert, Malika Kanodia, John A. Kvinge, Andrew Moran, and Jay Reding.

TABLE OF CONTENTS

§ 13.1 INTRODUCTION ... 13-1
§ 13.2 DEVELOPMENT OF PRIVACY TORT ... 13-1
- A. Common Law ... 13-1
- B. Constitutional Right ... 13-2
- C. Damages ... 13-4

§ 13.3 INVASION OF PRIVACY BY APPROPRIATION ... 13-4
- A. Requires Intent to Benefit ... 13-5
- B. Affirmative Defenses ... 13-5
  1. Consent ... 13-5
  2. Individual Not Identified ... 13-5
  3. Standing ... 13-6

§ 13.4 INTRUSION UPON SECLUSION ... 13-6
- A. Requirements to Prove ... 13-6
  1. Intent to Intrude ... 13-6
  2. Highly Offensive to a Reasonable Person ... 13-7
  3. Reasonable Expectation of Privacy ... 13-7
- B. Affirmative Defenses ... 13-8
  1. Public Property ... 13-8
  2. Consent ... 13-8
  3. Common Custom ... 13-9
  4. Waiver ... 13-9
  5. Third Party ... 13-9
- C. Claims Against the Government ... 13-9
- D. Statute of Limitations ... 13-9

§ 13.5 INVASION OF PRIVACY BY PUBLIC DISCLOSURE ... 13-10
- A. Requirements to Prove ... 13-10
  1. Publicity ... 13-10
  2. Truth ... 13-11
  3. Offensive to Reasonable Person ... 13-11
- B. Affirmative Defenses ... 13-12
  1. Public Benefit/Interest ... 13-12
  2. Newsworthiness ... 13-12
  3. Consent ... 13-13
  4. Qualified Privilege ... 13-13
  5. Event Took Place in Public ... 13-13

§ 13.6 INVASION OF PRIVACY BY FALSE LIGHT ... 13-13
- A. Requirements to Prove ... 13-14
  1. Publicity ... 13-14
  2. Highly Offensive to a Reasonable Person ... 13-14
- B. Affirmative Defenses ... 13-14
  1. Truth ... 13-14
  2. Public Interest ... 13-15
  3. Not Offensive to Ordinary Persons ... 13-15

4. No Malice ... 13-15
5. Waiver ... 13-16
6. Consent ... 13-16
§ 13.7 STATE AND FEDERAL STATUTES ... 13-16
A. HIPAA, 42 U.S.C. § 1301 *et seq.* ... 13-17
B. Financial Services Modernization Act (GLBA), 15 U.S.C. §§ 6801–6827 ... 13-18
C. Additional Prominent Federal Privacy Laws ... 13-19
D. State Statutes on Internet Privacy ... 13-20
§ 13.8 CONCLUSION ... 13-21

§ 13.1 INTRODUCTION

Over a century ago, two Harvard law students wrote a law review article following the history of tort law with regard to protections for personal injury as well as property damage. The authors, in their article entitled *The Right to Privacy*, considered "whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual[.]" Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193–220 (1890). Warren and Brandeis postulated that such a right should be protected by tort law.

Over time, the common law right to privacy developed into four basic torts as set out by Prosser in the *Restatement (Second) of Torts* §§ 652A–652I (1977):

- intrusion upon seclusion,
- appropriation,
- public disclosure of private facts, and
- false light publicity.

These individual torts are addressed in detail below. As the Minnesota Supreme Court recognized, however,

> [t]he common law is not composed of firmly fixed rules. Rather ... [it] is the embodiment of broad and comprehensive unwritten principles, inspired by natural reason, an innate sense of justice, adopted by common consent for the regulation and government of the affairs of men. It is the growth of ages, and an examination of many of its principles . . . discloses a constant improvement and development in keeping with advancing civilization and new conditions of society.

Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 233 (Minn. 1998) (citing *State ex rel. City of Minneapolis v. St. Paul, M. & M. Ry. Co.*, 108 N.W. 261, 268 (Minn. 1906)).

As technological advances have been made, the number of ways in which one's privacy can be invaded has increased exponentially, and the ability to broadcast such privacy invasions has become both instantaneous and global. As technological advances continue, consistent with the Minnesota Supreme Court's reminder that the common law "discloses a constant improvement and development in keeping with advancing civilization," the common law right to privacy will continue to develop and change. *Id.*

Now recognized in most jurisdictions, the right of privacy:

> has two main aspects: (1) the general law of privacy, which affords a tort action for damages resulting from an unlawful invasion of privacy, and (2) the constitutional right of privacy, which protects personal privacy against unlawful governmental invasion. The general law of the right of privacy, as a matter of tort law, is mainly left to the law of the states. . . .

Renwick v. News & Observer Publ'g Co., 312 S.E.2d 405, 411 (N.C. 1984), *cert. denied*, 469 U.S. 868 (1984).

§ 13.2 DEVELOPMENT OF PRIVACY TORT

A. Common Law

The basic concept of the right "to be left alone" in United States legal history can be traced all the way back to the United States Supreme Court case *Wheaton v. Peters*, 33 U.S. 591, 634 (1834) ("defendant asks noth-

ing—wants nothing, but to be let alone until it can be shown that he has violated the rights of another."). Warren and Brandeis relied upon this concept in their *Right to Privacy* article, and Brandeis subsequently used it in his dissent in *Olmstead v. U.S.*, 277 U.S. 438, 478 (1928), describing it as "the most comprehensive of rights and the right most valued by civilized men." The Georgia Supreme Court, however, was the first to expressly declare the existence of a common law "right to privacy" capable of being invaded. *See Pavesich v. New England Life Ins. Co.*, 50 S.E. 68, 80 (Ga. 1905) (finding that the "right of privacy has its foundation in the instincts of nature," and is therefore an "immutable" and "absolute right" derived from natural law).

Most states have recognized some or all of Prosser's four privacy torts at various times in the last few decades. These torts were not recognized in Minnesota until 1998, when the Minnesota Supreme Court held in the *Lake v. Wal-Mart Stores* case that Minnesota recognized the privacy torts of appropriation, intrusion upon seclusion, and public disclosure. Chief Justice Blatz wrote that, "[w]e decline to recognize the tort of false light publicity at this time. We are concerned that claims under false light are similar to claims of defamation, and to the extent that false light is more expansive than defamation, tension between this tort and the First Amendment is increased." *Lake*, 582 N.W.2d at 235. Prior to *Lake*, Minnesota was not held to have a common law right to claim an invasion of privacy. *See Berg v. Minneapolis Star & Tribune Co.*, 79 F. Supp. 957 (D. Minn. 1948) (holding Minnesota had no invasion of privacy protection under statute or common law); *Hendry v. Conner*, 226 N.W.2d 921 (Minn. 1975) (holding the law of Minnesota had never recognized a cause of action for invasion of privacy). As noted by the Minnesota Supreme Court in *Lake*, however, the "invasion of privacy" tort is recognized by the majority of jurisdictions. *Lake*, 582 N.W.2d at 235.

According to J. Thomas McCarthy, *The Rights of Publicity and Privacy* (2014 ed.), courts have "almost uniformly" adopted the four distinct torts that comprise the general right of privacy. Some states, like New York, opted to codify a right to protection from invasion of privacy.

> While the courts of other jurisdictions have adopted some or all of these torts, in this State the right to privacy is governed exclusively by sections 50 and 51 of the Civil Rights Law; we have no common law of privacy. . . . Balancing the competing policy concerns underlying tort recovery for invasion of privacy is best left to the Legislature, which in fact has rejected proposed bills to expand New York law to cover all four categories of privacy protection.

Talmor v. Talmor, 712 N.Y.S.2d 833, 836 (N.Y. Sup. Ct. 2000).

The invasion of privacy tort, even if codified by state statute, generally does not apply to corporations. "We have said that [the Massachusetts statute on an individual's right against interference with privacy] protects against the 'disclosure of facts about an individual that are of a highly personal or intimate nature.' . . . A corporation is not an 'individual' with traits of a 'highly personal or intimate nature.' Cases from other jurisdictions unanimously deny a right of privacy to corporations." *Warner-Lambert Co. v. Execuquest Corp.*, 691 N.E.2d 545, 548 (Mass. 1998) (citations omitted).

B. Constitutional Right

The Fourth Amendment also protects an individual's right to privacy, but this right is limited to the most intimate aspects of human affairs. Both rights to privacy (Fourth Amendment and common law) require a reasonable expectation of privacy. The Fourth Amendment right does not undermine the common law tort right:

> It is true that claims arising under either the Fourth Amendment or the tort of intrusion upon seclusion involve a violation of one's right of privacy. *See*, *e.g.*, *In re Asia Global Crossing,*

> *Ltd.*, 322 B.R. 247 (Bankr. S.D.N.Y. 2005) ("[A] right of privacy is recognized under both the common law, see RESTATEMENT (SECOND) OF TORTS 652B (1977) (discussing the tort of 'intrusion upon seclusion'), and the Fourth Amendment to the United States Constitution. In both cases, the aggrieved party must show a reasonable expectation of privacy.") (citations omitted). However, claims under these disparate provisions are distinct in kind and are not mutually exclusive.

DeBlasio v. Pignoli, 918 A.2d 822, 830 n.3 (Pa. Commw. 2007) (Kelly, dissenting).

However, "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'" *Katz v. United States*, 389 U.S. 347, 350 (1967). Indeed, these two privacy rights are not equal:

> The constitutional right of privacy is not to be equated with the common law right recognized by state tort law. Thus far only the most intimate phases of personal life have been held to be constitutionally protected. . . . Applying this limited doctrine of constitutional privacy, the federal courts have generally rejected efforts by plaintiffs to constitutionalize tortious invasions of privacy involving less than the most intimate aspects of human affairs.

McNally v. Pulitzer Publ'g Co., 532 F.2d 69, 70–71 (8th Cir. 1976) (abrogated in part on other grounds).

As with common law rights, the Fourth Amendment right to privacy requires a reasonable expectation of privacy, and there is no reasonable expectation of privacy when the information is in the public record. *Id*. at 77 ("Whatever the scope of the constitutional right of privacy in terms of the dissemination of information by one person regarding another person, it is clear that 'the interests in privacy fade when the information involved already appears on the public record.'").

The Federal Tort Claims Act (FTCA), which generally permits suits against the United States for torts committed by its agents, provides for a discretionary-function exception which precludes government liability for certain acts. The exception does not apply, however, to allegations of violations of constitutional rights. *See* 28 U.S.C. § 2680(a) (defining "discretionary-function exception" to FTCA); *Pooler v. United States*, 787 F.2d 868, 871 (3d Cir. 1986), *cert. denied*, 479 U.S. 849 (1986) (noting that discretionary-function exception would not apply if complaint alleged that federal agents violated plaintiff's constitutional rights in course of investigation, because federal agents do not possess discretion to commit such violations).

As such, government actors may receive qualified immunity from claims of invasion of privacy when such actions do not violate clearly established law:

> The threshold inquiry in a qualified immunity analysis decided on a motion for summary judgment is whether the plaintiff has alleged facts sufficient to establish a constitutional violation. This inquiry is made first so that even if the right asserted is not clearly established, a determination that it was violated might 'set forth principles which will become the basis for a holding that a right is clearly established.'
>
> . . . 'This is not to say that an official action is protected by qualified immunity unless the very action in question has previously been held unlawful; but it is to say that in the light of preexisting law the unlawfulness must be apparent.'

Hill v. McKinley, 311 F.3d 899, 902–04 (8th Cir. 2002) (citations omitted).

C. Damages

One who has established a cause of action for invasion of privacy is entitled to recover damages for:

(a) the harm to his or her interest in privacy resulting from the invasion;

(b) his or her mental distress proved to have been suffered if it is of a kind that normally results from such an invasion; and

(c) special damage of which the invasion is a legal cause.

See Restatement (Second) of Torts § 652H (1977).

COMMENT

> A cause of action for invasion of privacy, in any of its four forms, entitles the plaintiff to recover damages for the harm to the particular element of his privacy that is invaded. Thus one who suffers an intrusion upon his solitude or seclusion, under § 652B, may recover damages for the deprivation of his seclusion. One whose name, likeness or identity is appropriated to the use of another, under § 652C, may recover for the loss of the exclusive use of the value so appropriated. One to whose private life publicity is given, under § 652D, may recover for the harm resulting to his reputation from the publicity. One who is publicly placed in a false light, under § 652E, may recover damages for the harm to his reputation from the position in which he is placed.

Restatement (Second) of Torts § 652H (1977). Additionally, a plaintiff may also recover damages for emotional distress or special damages which can be proven.

While parties may restrict their damages within a contract, such limitations do not always apply to tort claims. Even if a corporate entity included a cap on damages and/or other limitation of liability provision in its contract with an individual, if the corporate entity was regulated under either HIPAA or the Gramm-Leach-Bliley Act (GLBA), the obligations to meet those statutory standards would still exist. The reason is that both of these privacy statutes were enacted to create a self-enforcement mechanism for regulated entities. The entity is responsible for establishing its own privacy and security policies and these two regulations hold them responsible for the obligations in those policies with respect to personally identifiable information or protected health information of the consumers.

§ 13.3 INVASION OF PRIVACY BY APPROPRIATION

The tort of invasion of privacy by appropriation was first recognized by the Minnesota Supreme Court in 1998. *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231 (Minn. 1998). Since then, the case law in Minnesota courts has not been significantly developed. *Wagner v. Gallup, Inc.*, 989 F. Supp. 2d 782, 791 (D. Minn. 2013). While appropriation generally means using another's name or likeness for one's own use or benefit, Minnesota has held that such a right to privacy has "not been extended beyond the protection of celebrities because a 'celebrity's property interest

in his name and likeness is unique.'" *Uhlaender v. Henricksen*, 316 F. Supp. 1277, 1283 (D. Minn. 1970); *see also*, RESTATEMENT SECOND OF TORTS § 652C (1977).

The Fifth Circuit held:

> Tortious liability for appropriation of a name or likeness is intended to protect the value of an individual's notoriety or skill. * * * [T]he appropriation tort does not protect one's name per se; rather, it protects the value associated with that name.

Kovatovich v. K-Mart Corp., 88 F. Supp. 2d 975, 986 (D. Minn. 1999) (citing *Matthews v. Wozencraft*, 15 F.3d 432, 437 (5th Cir. 1994)).

A. Requires Intent to Benefit

The invasion of privacy through appropriation requires that the defendant intended to benefit from such use, but such intent does not need to be pecuniary. Citing the *Restatement (Second) of Torts*, the Minnesota Supreme Court held that appropriation applies "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 in not a pecuniary one." *Faegre & Benson, LLP v. Purdy*, 367 F. Supp. 2d 1238, 1247–48 (D. Minn. 2005) (citations omitted); *see also Wagner*, 989 F. Supp. 2d at 791; *Ventura v. Kyle*, Civ. No. 12-472, 2012 WL 6634779, at *3 (D. Minn. Dec. 20, 2012).

The use of a name or likeness, without an intention to benefit, is not protected by the tort of appropriation. *See* RESTATEMENT SECOND OF TORTS § 652C, cmt. d (1977). Therefore, incidental use is not protected. *Kovatovich*, 88 F. Supp. 2d at 987 (citations omitted). Additionally, appropriation claims cannot involve a defendant who appropriates a plaintiff's name for a newsworthy purpose. *Id*.

B. Affirmative Defenses

1. Consent

Consent is an affirmative defense. However, a public performance does not necessarily translate into consent. A tort action for appropriation may be maintained for a broadcast of a person's image despite the fact that the performance was in public. *Zacchini v. Scripps-Howard Broad. Co.*, 433 U.S. 562 (1977) (holding broadcast of the whole public performance of a "human cannonball" without consent could be tried under an invasion of privacy tort claim).

However, the courts have held that even though a plaintiff voluntarily provides private information, consent may then be withdrawn so long as the revocation is given sufficiently in advance of publication. *Virgil v. Time, Inc.*, 527 F.2d 1122, 1126 (9th Cir. 1975), *cert. denied*, 425 U.S. 998 (1976).

2. Individual Not Identified

An action for appropriation requires use of a name or likeness which identifies the individual. An affirmative defense is that the "appropriation" does not name the individual.

However, even if the individual is not identified, an action for appropriation may be maintained if a pseudonym identifies the individual. *Faegre*, 367 F. Supp. 2d at 1248 (citing *McFarland v. Miller*, 14 F.3d 912, 922 (3d Cir. 1994) (holding New Jersey law prohibits appropriation of a celebrity's nickname)); *Ackerman v. Ferry*, No.

B143751, 2002 WL 31506931, at *18–19 (Cal. Ct. App. Nov. 12, 2002) (holding that California's appropriation statute covered appropriation of pseudonyms because "[n]icknames and pen names are names"); *Hirsch v. S.C. Johnson & Son, Inc.*, 280 N.W.2d 129, 137 (Wis. 1979) (holding that plaintiff stated a prima facie case for common law appropriation of his well-known nickname, Crazylegs, because "[a]ll that is required is that the name clearly identify the wronged person").

Even a slogan or catch-phrase may be sufficient to "identify" the individual and give rise to a claim of appropriation. *See Carson v. Here's Johnny Portable Toilets*, 698 F.2d 831, 835 (6th Cir. 1983) (recognized catch-phrase as identifiable attribute considered part of celebrity's right of publicity. "If the celebrity's identity is commercially exploited, there has been an invasion of the right whether his name or likeness is used.").

3. Standing

The individual claiming appropriation must have standing to make the claim. As noted earlier, a corporation may not claim an invasion of privacy based on appropriation. An employer, however, has standing to assert the collective privacy rights of its employees. *Faegre & Benson, LLP v. Purdy*, 447 F. Supp. 2d 1008, 1018 (D. Minn. 2006) (citing *Minneapolis Fed'n of Teachers, AFL-CIO, Local 59 v. Minneapolis Pub. Schs., Special Sch. Dist. No. 1*, 512 N.W.2d 107, 109–10 (Minn. Ct. App. 1994)).

§ 13.4 INTRUSION UPON SECLUSION

The invasion of privacy by intrusion upon seclusion can result not only from physical intrusion, but also through electronic or mechanical intrusion (i.e., wiretap or video surveillance). There must be secret or private matter which is obtained through unreasonable means. The tort of intrusion upon seclusion is defined by Prosser in the *Restatement (Second) Of Torts* § 652B as, "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." *See also Fletcher v. Price Chopper Foods of Trumann, Inc.*, 220 F.3d 871, 875 (8th Cir. 2000).

A. Requirements to Prove

1. Intent to Intrude

Intent, the first element of a claim of intrusion upon seclusion, has not been extensively discussed by Minnesota courts. The *Restatement* defines "intent" as meaning that "the actor desires to cause consequences of his act, or that he believes the consequences are certain to result from it." RESTATEMENT (SECOND) OF TORTS § 8A (1977). Relying on this definition, courts in several jurisdictions have held that accidental or unintentional intrusions upon seclusion are not actionable. *See*, *e.g.*, *O'Donnell v. United States*, 891 F.2d 1079, 1083 (3d Cir. 1989). The Eighth Circuit Court of Appeals explained that actionable intrusion requires that the defendant "believes, or is substantially certain, that he lacks the necessary legal or personal permission to commit the intrusive act." *Fletcher v. Price Chopper Foods of Trumann, Inc.*, 220 F.3d 871, 876 (8th Cir. 2000).

The intent to intrude requires: (1) the existence of a secret and private subject matter, (2) the plaintiff's right to keep that subject matter private, and (3) the obtainment by the defendant of information about that subject matter through unreasonable means (e.g., eavesdropping or spying). *Thomas v. Corwin*, 483 F.3d 516, 531 (8th Cir. 2007); *see also* RESTATEMENT (SECOND) OF TORTS § 652B, cmt. b (1977) (adopted by Minnesota Supreme Court in *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 235 (Minn. 1998)). On the requirement of the use of "unreasonable means," the Eighth Circuit reasoned: "[a] plaintiff cannot establish the defendant's use of 'unreasonable means' to

obtain information if a defendant obtains such information in the ordinary course of business or in response to a discovery request during litigation.” *Thomas*, 483 F.3d at 532.

2. Highly Offensive to a Reasonable Person

Not all intrusions are actionable. The second element of the claim requires the intrusion to rise to the level of being “highly offensive to a reasonable person.” *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 233 (Minn. 1998).

While the ultimate determination of whether an intrusion is “highly offensive” is a fact question for a jury, Minnesota courts will make a preliminary determination of “offensiveness” before allowing the claim to proceed to a jury. *Bauer v. Ford Motor Credit Co.*, 149 F. Supp. 2d 1106, 1109 (D. Minn. 2001). Factors to be considered by the court include:

> The degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder’s motives and objectives, the setting into which he intrudes, and the expectation of those whose privacy is invaded.

Id. “The question of what kinds of conduct will be regarded as ‘highly offensive’ intrusion is largely a matter of social conventions and expectations.” *Id.* However, the factual inquiry into “offensiveness” becomes purely legal “if reasonable persons can draw only one conclusion from the evidence.” *Swarthout v. Mut. Serv. Life Ins. Co.*, 632 N.W.2d 741, 745 (Minn. Ct. App. 2001).

The inquiry into offensiveness has been described as “analogous to the ‘shock the conscience’ analysis employed in substantive Due Process claims.” *Andersen v. Cnty. of Becker*, Civ. No. 08-5687, 2009 WL 3164769, at *14 (D. Minn. Sept. 28, 2009). Other courts have described the claim as requiring “an objectively-based threshold degree of ‘repugnance.’” *Fabio v. Credit Bureau of Hutchinson, Inc.*, 210 F.R.D. 688 (D. Minn. 2002).

3. Reasonable Expectation of Privacy

Minnesota requires the individual claiming intrusion upon seclusion to have a reasonable expectation of privacy in the subject matter intruded upon. An individual does not have a “reasonable” expectation of privacy for information which is otherwise public. *See Phillips v. Grendahl*, 312 F.3d 357 (8th Cir. 2002). Information contained on a driver’s license, including height, weight, eye color, and address, has been held not to be the type of information for which an individual may have a reasonable expectation of privacy, since driver’s licenses are shown to strangers on a daily basis. *See*, *e.g.*, *Mallak v. Aitkin Cnty.*, 9 F. Supp. 3d 1046, 1064 (D. Minn. 2014).

Whether a plaintiff must be physically present for the intrusion to plead a valid claim is fact-specific. In *Hays v. Citimortgage, Inc.*, Civ. No. 11-2477, 2012 WL 1319413 (D. Minn. Mar. 29, 2012), the district court concluded that it is not a defense to such a claim to say the plaintiff was not present during the intrusion, citing *Ford Motor Co. v. Williams*, 132 S.E.2d 206, 211–12 (Ga. Ct. App. 1963), *rev’d on other grounds by* 134 S.E.2d 32 (Ga. 1963) (specifically addressing “whether there can be an invasion of plaintiff’s privacy by entering his home when no one was at home,” and finding a cause of action for intrusion of seclusion when defendant’s employees entered plaintiff’s home to recover allegedly stolen property while plaintiff was not at home, and urinated on his property) and *Gonzales v. Southwest Bell Telephone Co.*, 555 S.W.2d 219, 223 (Tx. Ct. App. 1977) (rejecting defendant’s argument that no cause of action existed for an invasion of privacy resulting from an entry into a person’s home when the person was not present).

While Minnesota courts have yet to fully delineate the contours of this tort, the *Restatement* specifically mentions surreptitious recording of telephone conversations as an example of the tort of intrusion upon seclusion. Restatement (Second) Of Torts § 652B, cmt. b & illus. 3 (1977). Note, however, that many state laws, including those in Minnesota and Wisconsin, do not prohibit secret recordings of conversations as long as at least one party to the conversation is aware of the recording and consents. Other states, including Illinois and California, require the consent of all parties to the conversation. In *Milke v. Milke*, No. 03-CV-6203, 2004 WL 2801585, at *4 (D. Minn. June 14, 2004), which held that a husband's secret recordings of his wife's calls constituted an actionable intrusion upon seclusion, none of the parties to the telephone calls knew they were being recorded.

A recent area of dispute concerns employee expectations of privacy in work email accounts. Courts are split over the issue, with some concluding that employees have no expectation of privacy when using an employer email system (e.g., *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 100–01 (E.D. Pa. 1996)), while others have found an expectation of privacy where an employee accesses a personal webmail account using a company computer (*Convertino v. U.S. Dep't of Justice*, 674 F. Supp. 2d 97, 110 (D.D.C. 2009)). In an unpublished decision, the Minnesota Court of Appeals chose a middle ground by adopting a four-part test to measure the expectation of privacy. *Gates v. Wheeler*, No. A09-2355, 2010 WL 4721331 (Minn. Ct. App. Nov. 23, 2010). The test asks the following questions: "(1) is there a corporate policy; (2) does the company monitor employee email use; (3) do third parties have a right of access; and (4) did the corporation notify the employee or did the employee know about the use and monitoring policies?" *Id.*, at *6 (citing *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005)).

Similar concerns have been raised about privacy in social media accounts. *See R.S. v. Minnewaska Area Sch. Dist. No. 2149*, 894 F. Supp. 2d 1128, 1142 (D. Minn. 2012) ("The Court agrees that one cannot distinguish a password-protected private Facebook message from other forms of private electronic correspondence.").

B. Affirmative Defenses

1. Public Property

If the alleged "intrusion" was done on public property, it is likely that the claim of invasion of privacy will fail. The Ninth Circuit held that the publication of a videotape made in a public place was a valid defense to the claim of intrusion upon seclusion where only a brief clip was played and no personal details were reported. *Deteresa v. Am. Broad. Cos., Inc.*, 121 F.3d 460, 461, 465 (9th Cir. 1997), *cert. denied*, 523 U.S. 1137 (1998). The *Restatement (Second) of Torts* echoes this concept, describing that it may be permissible to take a photograph of a person walking on a public highway, as they would not be "in seclusion" but cautioning: "Even in a public place, however, there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze." Restatement (Second) of Torts § 625B, cmt. c (1977).

2. Consent

Consent is also an affirmative defense to the claim of intrusion upon seclusion. *Cox v. Hatch*, 761 P.2d 556, 563–64 (Utah 1988) (holding consent to a photograph precluded a claim of intrusion upon seclusion).

However, the courts have held that even though a plaintiff voluntarily provides private information to a reporter, consent to publication may be subsequently withdrawn so long as the revocation is given sufficiently in advance of publication, and provided the information to be published is "not of legitimate concern to the public." *Virgil v. Time Inc.*, 527 F.2d 1122, 1126 (9th Cir. 1975).

In *Dubbs v. Head Start, Inc.*, 336 F.3d 1194, 1219 (10th Cir. 2003), the court held that consent can be inferred from industry custom and dismissed claims for intrusion upon seclusion brought against nurses who were told that the parents of students they examined had consented to the examinations. The undisputed evidence established that it was the custom in the industry to rely on assurances from other health care professionals that proper consent had been obtained.

3. Common Custom

Any intrusion which is deemed to be customary or common usage is not actionable. When a reporter took a photograph of a fire victim at the request of the fire marshal that had run out of film, the Florida Supreme Court held there was no invasion of privacy because it is customary for reporters to accompany public officials to disaster scenes. *Florida Publ'g Co. v. Fletcher*, 340 So. 2d 914 (Fla. 1976), *cert. denied*, 431 U.S. 930 (1977). *See also Dubbs*, 336 F.3d at 1219.

4. Waiver

The right to have one's privacy protected by not allowing intrusion upon seclusion is a right which may be waived. Similar to consent, a waiver is a voluntary and intentional relinquishment or abandonment of a known right. *Montgomery Ward & Co. v. Cnty. of Hennepin*, 450 N.W.2d 299, 304 (Minn. 1990). A plaintiff may waive his or her right to privacy through conduct manifesting a clear intent to do so. *Milke v. Milke*, No. 03-CV-6203, 2004 WL 2801585, at *4 (D. Minn. June 14, 2004) (citing *Anderson v. Low Rent Housing Comm'n of Muscatine*, 304 N.W.2d 239, 249 (Iowa 1981) (limited public statements not a waiver); *Black v. City and Cnty. of Honolulu*, 112 F. Supp. 2d 1041, 1053–54 (D. Haw. 2000) (being friendly to surveillance officers not a waiver)). The defendant bears the burden of proof on waiver. *Black*, 112 F. Supp. 2d at 1054.

5. Third Party

In a claim of intrusion upon seclusion alleging that the defendant was liable for the actions of a third party who carried out the actual intrusion, the defendant claimed as a defense that he could not be held liable because he personally did not intrude. *Radford v. Miller*, No. A11-298, 2012 WL 1380262 (Minn. Ct. App. Apr. 23, 2012). The Minnesota Court of Appeals held that because the intrusion was done at the express direction of the defendant, the district court's ruling not to grant a motion for judgment as a matter of law was upheld. *Id*.

C. Claims Against the Government

While the FTCA, 28 U.S.C. §§ 2671–2680, allows tort claims to be brought against the government, it expressly provides exceptions for certain tort claims for which the government may not be held liable. 28 U.S.C. § 2680. The Eighth Circuit Court of Appeals has held that the tort of intrusion upon seclusion is not one of the exceptions to the general waiver of sovereign immunity, and has allowed claims for intrusion upon seclusion to proceed against the federal government. *Raz v. U.S.*, 343 F.3d 945 (8th Cir. 2003). *But see* 28 U.S.C. § 2680(a) (government not liable for exercise of statute or regulation or performance of discretionary function as long as due care was used).

D. Statute of Limitations

Claims for intrusion upon seclusion are subject to a two-year statute of limitations. MINN. STAT. § 541.07; *Hough v. Shakopee Pub. Schs.*, 608 F. Supp. 2d 1087, 1118 (D. Minn. 2009).

§ 13.5 INVASION OF PRIVACY BY PUBLIC DISCLOSURE

The invasion of privacy by public disclosure is the publication of non-newsworthy, private facts about an individual that would be highly offensive to a reasonable person. *See* RESTATEMENT (SECOND) OF TORTS § 652D (1977) ("One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that: (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.").

A. Requirements to Prove

1. Publicity

The invasion of privacy by publication requires 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." *Tureen v. Equifax, Inc.*, 571 F.2d 411, 417 (8th Cir. 1978) (citing RESTATEMENT (SECOND) OF TORTS § 625D, cmt. (1977)). Merely communicating something to a third party does not constitute the "publicity" required for this tort.

Posting private information in a shop window constitutes "publicity" according to the *Restatement* approach. RESTATEMENT (SECOND) OF TORTS § 267, cmt. a, illus. 2 (1977). *See also Brents v. Morgan*, 299 S.W. 967, 968, 971 (Ky. 1927) (exemplifying "publicity" under the *Restatement*, posting a 5-by-8 foot notice calling attention to a customer's overdue account in a show window of an automobile garage constitutes publicity); *Biederman's of Springfield, Inc. v. Wright*, 322 S.W.2d 892, 898 (Mo. 1959) (holding that loud declarations of indebtedness in a public restaurant constituted "publicity").

Additionally, "the majority of state and federal courts to consider this issue have held that communication to a few people is not sufficient publicity to state a cause of action under this [public disclosure] tort." *C.L.D. v. Wal-Mart Stores, Inc.*, 79 F. Supp. 2d 1080, 1084 (D. Minn. 1999) (citations omitted). Minnesota courts have followed this rule, and adopted the *Restatement* approach in defining what constitutes "publicity:"

> We conclude, therefore, that "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." RESTATEMENT (SECOND) OF TORTS § 652D cmt. a. In doing so, we have considered whether there are legitimate or compelling reasons of public policy that justify imposing liability for egregious but limited disclosures of private information. We conclude, nevertheless, that the Restatement's publicity requirement best addresses the invasion of privacy cause of action--absent dissemination to the public at large, the claimant's "private persona" has not been violated.

Bodah v. Lakeville Motor Express, Inc., 663 N.W.2d 550, 557–58 (Minn. 2003) (citation omitted). The *Bodah* case overruled a prior decision of the Minnesota Court of Appeals that held that disclosure of employee names and Social Security numbers to 16 managers in six states constituted "publicity." *Id*. The Minnesota Supreme Court held that this was insufficient to constitute "publicity" as required under the *Restatement* approach.

If the element of publicity cannot be shown, a court does not need to address the other elements. *Robins v. Conseco Fin. Loan Co.*, 656 N.W.2d 241, 246 (Minn. Ct. App. 2003).

With the rise of the Internet, it is even easier to post private information in a way that constitutes "publicity." For instance, in *Yath v. Fairview Clinics, N.P.*, 767 N.W.2d 34, 43 (Minn. Ct. App. 2009) the Minnesota Court

of Appeals drew an analogy between a posting on the social media site MySpace as being similar to a posting made in a shop window. With social media, the opportunities for publication of private information have dramatically increased. However, the *Yath* decision involved a posting that was entirely public. *Yath*, 767 N.W.2d at 45. If private facts are posted on a non-public site (e.g. a Facebook page only accessible to a limited number of people), it is possible that there would not be sufficient "publicity" under the *Restatement* approach.

Likewise, posting private data such as Social Security numbers may constitute a tort under the *Restatement* approach. The Ninth Circuit explained the nature of Social Security numbers and recognized that their uniqueness lends itself to abuse if disclosed. *In re Crawford*, 194 F.3d 954, 958 (9th Cir. 1999). In *Bodah*, the Minnesota Supreme Court concluded in dicta that had the employee information, including Social Security numbers, been posted publicly rather than to a small group, the outcome of the case could have been different. *Bodah*, 663 N.W.2d at 559 (citing an unpublished Minnesota federal district court case). *See also*, *Meyerson v. Prime Realty Servs., LLC*, 796 N.Y.S.2d 848, 912 (N.Y. Sup. 2005) (holding that "in relation to a private transaction, this court may well adopt a bright line standard that a social security number is prima facie privileged information, with the privilege to be asserted only after the demanding party demonstrates entitlement to confidential information. While the privilege must give way as required by statute, regulation or court order, in ordinary circumstances, the person who holds the social security number appears to be free to decline disclosure.").

Additionally, private information required for the performance of a service or in the normal course of business is not likely to be deemed "publicity" for purposes of a tort claim for invasion of privacy:

> [T]he communication of information to other insurers is not equivalent to a communication to the general public or to a communication to a group of persons large enough to permit the matter to be regarded as substantially certain to become one of public knowledge. In the absence of such undue publicity there is no actionable violation. . . .

Wilson v. Colonial Penn Life Ins. Co., 454 F. Supp. 1208, 1213 (D. Minn. 1978) (citing Restatement (Second) of Torts § 652D, cmt. a (1971)).

2. Truth

The invasion of privacy by publication requires that the disclosed information be true. This element distinguishes this tort from the tort of defamation. *Lake*, 582 N.W.2d at 235.

3. Offensive to Reasonable Person

The protection afforded to the plaintiff's interest in his or her privacy must be relative to the customs of the time and place, to the occupation of the plaintiff, and to the habits of his or her neighbors and fellow citizens. If the disclosure would not be offensive to a "reasonable person" based on the plaintiff's own circumstances, then the action may not be maintained. Restatement (Second) of Torts § 652D, cmt. a (1971). However, even if a publication is true, it is not enough that it would be offensive to a reasonable person if the subject matter is a valid concern of the public. Restatement (Second) of Torts § 652D, cmt. b (1971).

B. Affirmative Defenses

1. Public Benefit/Interest

Publication of information that is a valid concern of the public does not constitute an invasion of privacy tort claim under publication.

> Permissible publicity (of) information concerning either voluntary or involuntary public figures is not limited to the particular events that arouse the interest of the public. That interest, once aroused by the event, may legitimately extend, to some reasonable degree, to further information concerning the individual and to facts about him, which are not public and which, in the case of one who had not become a public figure, would be regarded as an invasion of his purely private life. Thus, the life history of one accused of murder, together with such heretofore private facts as may throw some light upon what kind of person he is, his possible guilt or innocence, or his reasons for committing the crime are a matter of legitimate public interest.

Logan v. District of Columbia, 447 F. Supp. 1328, 1333 (D.D.C. 1978).

Broadcasting footage of the remains of an abducted child's skull did not support a private facts action by the child's family because the discovery of the remains was a matter of public interest. *Armstrong v. H & C Commc'ns Inc.*, 575 So. 2d 280 (Fla. Dist. Ct. App. 1991).

Where there were allegations of sexual harassment and falsified information on an employment application for a city employee present on an official public record, there was a legitimate public interest in the information that barred a claim for publication of private facts. *Mooers v. City of Lake City*, No. A13-2197, 2014 WL 3023368 (Minn. Ct. App. July 7, 2014).

2. Newsworthiness

The publication of a person's name or picture in connection with a news or historical event which is of a valid public interest does not constitute an actionable invasion of the right of privacy. A California appeals court analyzing the defense of newsworthiness stated that:

> while the general object in view is to protect the privacy of private life, nevertheless, 'to whatever degree and in whatever connection a person's life has ceased to be private, before the publication under consideration has been made, to that extent the protection is to be withdrawn.' In connection with what constitutes news regarding matters of public or general concern, it is said in *Associated Press v. International News Service*, that news is said to have 'that indefinable quality of interest, which attracts public attention'; while the court in *Jenkins v. News Syndicate Co.*, defines news as a 'report of recent occurrences.'

Metter v. Los Angeles Examiner, 95 P.2d 491, 496 (Cal. Ct. App. 1939) (citations omitted); *see also Hurley v. Nw. Publ'ns, Inc.*, 273 F. Supp. 967, 976 (D. Minn. 1967) (quoting *Metter*).

"One's private affairs may wittingly or unwittingly become public, as often happens when litigation ensues." *Hurley*, 273 F. Supp. at 975 (citation omitted). The line between newsworthy and non-newsworthy is based on customs and community standards. *Virgil*, 527 F.2 at 1126.

3. Consent

The invasion of privacy by publication cannot be maintained if the publication was with consent. *Zacchini v. Scripps-Howard Broad. Co.*, 433 U.S. 562 (1977) (holding broadcast of the whole performance of a "human cannonball" without consent could be tried under an invasion of privacy tort claim.) *See also Rosko v. Times Publ'g Co. Inc.*, No. 90-016311-17, 1991 WL 324792 (Fla. Cir. Ct. Nov. 1, 1991).

However, the courts have held that even though a plaintiff voluntarily provides private information, consent may then be withdrawn so long as the revocation is given sufficiently in advance of publication. *Virgil v. Time, Inc.*, 527 F.2d 1122, 1127 (9th Cir. 1975).

4. Qualified Privilege

If a person injects himself or herself into a matter of public concern, it may constitute an affirmative defense of "qualified privilege." An Iowa case from 1961 held that "by interjecting himself into a matter of public concern and by criticizing the actions of public officials and requesting certain action had invited or at least excused comment and criticism from those who held other views." *Haas v. Evening Democrat Co.*, 107 N.W.2d 444 (Iowa 1961). *See also Rees v. O'Malley*, 461 N.W.2d 833, 838–39 (Iowa 1990) (holding that action did not rise to level of interjection into a matter of public concern).

5. Event Took Place in Public

Publication as a matter of public record of information about which the public has a valid concern does not constitute an invasion of privacy. *McNally v. Pulitzer Publ'g Co.*, 532 F.2d 69, 78–79 (8th Cir. 1976); *cf. Cox Broad. Corp. v. Cohn*, 420 U.S. 469 (1975) (holding information from public records is absolutely privileged); *see also Mooers*, 2014 WL 3023368, at *6 (disclosure was part of public information in city records).

A photograph taken in a public place does not constitute an invasion of privacy. *Heath v. Playboy Enters., Inc.*, 732 F. Supp. 1145 (S.D. Fla. 1990). It is possible, however that the commercial use of the image might still qualify as appropriation.

See also Machleder v. Diaz, 538 F. Supp. 1364 (S.D.N.Y. 1982), *aff'd in part, rev'd in part on other grounds*, 801 F.2d 46 (2d Cir. 1986) (holding that videotaping from a public entrance of a company is a semi-public area still visible to the public and therefore defensible).

§ 13.6 INVASION OF PRIVACY BY FALSE LIGHT

Although similar to libel or defamation, invasion of privacy by false light means publicity of private information with malice or with reckless disregard for the truth, thereby creating a deliberately false and misleading impression of a person that is highly offensive to a reasonable person. "Publicity placing person in false light" is defined by Prosser in the *Restatement Second of Torts* § 652E (1997) as:

> One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if[:] (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) 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.

The United States Supreme Court first considered the parameters of false light invasions of privacy in *Time, Inc. v. Hill*, 385 U.S. 374 (1967) (holding actual malice standard required as counter balance to First Amendment right to free speech).

Although this tort is not recognized in Minnesota, the Eighth Circuit has acknowledged this tort under Missouri law. *Gore v. Trans World Airlines*, 210 F.3d 944, 951 (8th Cir. 2000) (citing *Sullivan v. Pulitzer Broad. Co.*, 709 S.W.2d 475, 478 n.5 (Mo. 1986) (en banc)).

Nonetheless, states which have not expressly precluded this tort have not always incorporated it. For example:

> [i]n no case has a Florida appellate court affirmed a judgment for the plaintiff in a false light invasion of privacy case. And, with the apparent exception of the *Heekin* case, no Florida appellate court has upheld a complaint on the ground that it states a cause of action for invasion of privacy based on the false light theory.

Gannett Co., Inc. v. Anderson, 947 So. 2d 1 (Fla. Ct. App. 2006). On the other hand, some states have expressly included a false light tort. *West v. Media Gen. Convergence, Inc.*, 53 S.W.3d 640 (Tenn. 2001) (holding that "false light" should be recognized as a distinct, actionable tort).

A. Requirements to Prove

1. Publicity

As with the other privacy torts, a claim of false light invasion of privacy requires private information to be publicized. "The 'publicity' required for the invasion of privacy tort of false light publicity is identical to that required for publication of private facts." *Bodah v. Lakeville Motor Express Inc.*, 663 N.W.2d 550, 554 n.3 (citing Restatement (Second) of Torts § 652E, cmts. a & b, illus. 1–5 (1977)). Also, such information must be unreasonably obtained. *Gore*, 210 F.3d 944.

2. Highly Offensive to a Reasonable Person

The New Mexico Appellate Court held that a plaintiff "has shown facts from which a jury could conclude that he was placed in a 'false light . . . [that] would be highly offensive to a reasonable person.'" *Moore v. Sun Publ'g. Corp.*, 881 P.2d 735, 744 (N.M. Ct. App. 1994) (citing Restatement (Second) of Torts § 652E(a) (1977)); *see Larsen v. Philadelphia Newspapers, Inc.*, 543 A.2d 1181, 1189 (Pa. Super. Ct. 1988) (false light claim may be established where true information published if the information tends to imply falsehoods), *appeals denied*, 552 A.2d 251 (Pa. 1988), 552 A.2d 252 (Pa. 1988), 552 A.2d 968 (Pa. 1988), *cert. denied*, 489 U.S. 1096 (1989); *Jonap v. Silver*, 474 A.2d 800, 806 (Conn. Ct. App. 1984) (jury verdict sustained where there was evidence that defendants caused letter to be published in a magazine that attributed to plaintiff views that were not his own and that there was a major misrepresentation of his character, history, activities, or beliefs).

B. Affirmative Defenses

1. Truth

"The essential element of untruthfulness differentiates 'false light' from the other forms of invasion of privacy and many times affords an alternate remedy for defamation even though it is not necessary for a plaintiff to prove that he or she was defamed." *Anderson v. Low Rent Housing Comm'n*, 304 N.W.2d 239 (Iowa 1981).

While some courts require that the statement be untrue, *see Baker v. Burlington N., Inc.*, 587 P.2d 829 (Idaho 1978); *Rinsley v. Brandt*, 446 F. Supp. 850 (D. Kan. 1977); *Logan v. District of Columbia*, 447 F. Supp. 1328 (D.D.C. 1978) (no action if "substantially true"), a true statement may be actionable where it tends to imply a falsehood. *See Larsen*, 543 A.2d at 1189.

"Although in this category [of a "false light" tort] actual truth of statements is not necessarily an issue, a false impression relayed to the public, is." *McCormack v. Okla. Publ'g Co.*, 613 P.2d 737 (Okla. 1980).

The courts have the discretion to distinguish between slight inaccuracies and purposeful untruths:

> We agree with the appellant that minor inaccuracies and fictionalized dialogue will not alone defeat the privilege granted to truthful publications of public interest. . . . . The district court here, however, specifically instructed the jury to ignore minor inaccuracies and required them to find 'substantial' falsity. In light of the evidence outlined above and the unobjectionable instructions, we believe that the jury was entitled to accept plaintiff's view that the article as a whole presented a substantially false and distorted picture of him and his relationship with his wife.

Varnish v. Best Medium Publ'g Co., 405 F.2d 608 (2d. Cir. 1968) (citations omitted).

2. Public Interest

It is an affirmative defense against a claim of false light invasion of privacy to show a valid public interest in the information published. "With few exceptions, the cases hold that once a person's activities become a matter of public interest, he usually cannot revert to a private status." *McCormack*, 613 P.2d at 742.

3. Not Offensive to Ordinary Persons

A false light invasion of privacy claim must be based on a disclosure which is offensive to a reasonable person.

> Appellant also argues that there was no showing that the article was offensive to persons of ordinary sensibilities, as required by Pennsylvania law. Pennsylvania has held, however, in a case quite similar to this one, that this issue is peculiarly within the competence of the jury. . . . We cannot say as a matter of law that the Enquirer article would not be offensive to a person of ordinary sensibilities.

Varnish, 405 F.2d at 612 (citation omitted).

4. No Malice

Although the Supreme Court in *Time, Inc. v. Hill*, 385 U.S. 374 (1967) stated that malice must be shown, whether that malice must be actual or implied was not definitively decided.

> [T]he question of whether in false-light cases the plaintiff must allege and prove 'actual malice' has been left open. We conclude, however, in light of the admonition of *Leopold v. Levin* to proceed with caution, that in false-light cases it is not necessary to distinguish

> between private and public figures, as is required in some defamation cases, and we, accordingly, adopt the 'actual malice' approach of the Restatement.

Lovgren v. Citizens First Nat'l Bank of Princeton, 534 N.E.2d 987 (Ill. 1989). *See also Colbert v. World Publ'g Co.*, 747 P.2d 286 (Okla. 1987).

Whether or not malice can be shown through reckless disregard of the falsity of the information is not clear. The Tenth Circuit held that: "In order to establish reckless disregard, Plaintiff must demonstrate actual knowledge of probable falsity. 'The only extent that an investigation enters into the consideration of the premises is if the investigation is made and through it, actual knowledge is imparted.'" *Zeran v. Diamond Broad., Inc.*, 203 F.3d 714 (10th Cir. 2000).

5. Waiver

As with the other rights of privacy, a false light invasion of privacy claim may be waived.

> The right of privacy may be lost by express or implied waiver by the complaining party. . . . Waiver is generally defined as the voluntary and intentional relinquishment of a known right. . . . For implied waiver to exist, the intention of the party alleged to have waived his or her rights must be clear from the party's conduct. . . . Normally the question of waiver is one for the jury; however, where the evidence is not in dispute, the question becomes one of law for the court.

Anderson, 304 N.W.2d at 249 (citations omitted).

6. Consent

Consent is an affirmative defense to a false light invasion of privacy claim as it is with the other privacy torts. *Zacchini v. Scripps-Howard Broad. Co.*, 433 U.S. 562 (1977). However, the courts have held that, even though a plaintiff voluntarily provides private information, consent may then be withdrawn so long as the revocation is given sufficiently in advance of publication. *Virgil*, 527 F.2d at 1126.

§ 13.7 STATE AND FEDERAL STATUTES

Although the privacy tort law is based on common law, the explosion of security breaches in recent years has led to an expansion of state and federal privacy laws, regulations, and guidelines regulating the collection and use of personal data, which is becoming one of the fastest growing areas of legal regulation. In Minnesota, for example, there are statutes requiring persons or businesses that maintain data that includes individual personal information or "personally identifiable information" (PII) to protect the unauthorized acquisition or prohibited disclosure of PII, which includes but is not limited to the individual's identifying information such as a Social Security number, a driver's license number, account number, or a credit or debit card number. *See* MINN. STAT. §§ 325E.61 & 325M.01–325M.09. The Minnesota Health Records Act requires certain providers of health care services who maintain individual personal health records to protect the privacy of a patient's health records and forbids the providers from releasing health records to a third party without patient consent, unless an exception applies. MINN. STAT. §§ 144.291–144.298. Most states also have what is referred to as a "state sunshine law" which governs public access to governmental records and provides regulations for the acquisition and safekeeping of public and private data. These laws may apply to private parties. In Minnesota, for example, under the Minnesota Government Data Practices Act, MINN. STAT. § 13.01 *et seq.*, certain companies or individuals that contract with a government entity to perform one of the government entity's

functions is also subject to the provisions under the Minnesota Government Data Practices Act with respect to the data collected or created for that function. *See* MINN. STAT. § 13.05.

At the federal level, the United States has also enacted statutes that provide privacy protections for individuals, particularly when the information may be electronically transmitted. Many of the federal statutes apply to particular categories of personal information, such as financial or health information, or electronic communications, while others apply to activities that use personal information, such as telemarketing and commercial email. There are also broad consumer protection laws that, while not privacy laws per se, have been used to prohibit unfair or deceptive practices involving the disclosure of and security procedures for protecting personal information. Two primary data privacy statutes are aimed at regulated industries—health care providers and financial institutions. As to both industries, the initial concern was that, with the rise of the Internet and the ease of electronically transmitting information, these types of entities could potentially put their customers' private information at risk. The laws were drafted to provide guidelines for regulated entities of the minimum-security standard to protect "protected health information" (PHI) under the Health Insurance Portability and Accountability Act (HIPAA) for health care providers, or "personally identifiable information" (PII) under the Gramm-Leach-Bliley Act (GLBA) for financial institutions. These statutes are discussed in greater detail below.

Some federal laws preempt state privacy laws on the same topic, while there are many federal privacy laws that contain express provisions denying preemption of state laws that afford greater privacy protection to consumers. Consequently, compliance with both state and federal privacy laws that regulate the same types of data (such as, for example, maintaining the privacy of health records where compliance with both the Minnesota Health Records Act and HIPAA is necessary) or the same types of activities, may be required.

A. HIPAA, 42 U.S.C. § 1301 *et seq.*

The HIPAA regulates medical information and applies to covered entities. A "covered entity" is defined as a health plan, health care clearinghouse, or a health care provider that transmits any health information in electronic form in connection with a transaction covered by the subchapter. 45 C.F.R. § 160.103. HIPAA has various parts. The Privacy Rule applies to the collection and use of PHI. *See* 45 C.F.R. Parts 160 & 164. The privacy rules identify when PHI may be: (1) used or disclosed, (2) shared with others, (3) protected from unauthorized disclosure, and (4) the right of the individual to review and/or correct the information. The Security Rule provides standards for protecting medical data. *See* 45 C.F.R. Parts 160 & 164. The Transactions Rule applies to the electronic transmission of medical data. *See* 45 C.F.R. Parts 160 & 162. These HIPAA rules were revised in early 2013 under the HIPAA "Omnibus Rule." The Omnibus Rule also revised the Security Breach Notification Rule, 45 C.F.R. Part 164, which requires covered entities to provide notice of a breach of PHI.

HIPAA also applies to business associates. In general, when a covered entity enters into a business relationship with an outside person who has access to the covered entity's PHI (a "business associate"), the parties must enter into a contract to ensure that the business associate will appropriately safeguard the PHI and to clarify the permissible uses and disclosures of PHI by the business associate. A "business associate" is defined as a person who:

> (i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing

or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R. § 3.2, billing, benefit management, practice management, and reprising; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

45 C.F.R. § 160.103.

Examples of a business associate include:

- a third-party administrator that assists a health plan with claims processing;
- a CPA firm whose accounting services to a health care provider involve access to protected health information;
- an attorney whose legal services to a health plan involve access to protected health information;
- a consultant that performs utilization reviews for a hospital;
- a health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer;
- an independent medical transcriptionist that provides transcription services to a physician; or
- a pharmacy benefits manager that manages a health plan's pharmacist network.

See 45 C.F.R. § 160.103.

If a business associate contract is necessary, the contract must include the elements specified at 45 C.F.R. § 164.504(e). For example, among other things, the contract must describe the permitted and required uses of PHI by the business associate, provide that the business associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law, and require the business associate to use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the contract. Under 45 C.F.R. § 164.532(d) and (e), a covered entity can only make permissible disclosures to business associates. The United States Department of Health & Human Services provides sample business associate contract provisions on its website on "Business Associate Contracts" at <www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>. In addition, there are situations in which a business associate contract is not required such as, for example, with persons or organizations, such as janitorial service or electrician, whose functions or services do not involve the use or disclosure of protected health information, and where access to protected health information by such persons would be incidental. *See* 45 C.F.R. §§ 160.103 & 164.502(e).

B. Financial Services Modernization Act (GLBA), 15 U.S.C. §§ 6801–6827

The GLBA regulates the collection, use, and disclosure of non-public personal information collected by a financial institution that is provided by, results from, or is otherwise obtained in connection with their customers, and

in some cases their consumers who do not have an on-going relationship with the institution, who obtain financial products or services primarily for personal, family, or household purposes from a financial information. A "financial institution" is defined to include any institution engaging in financial activities, such as banks, securities firms, and insurance companies, and to other businesses that provide financial services and products. *See* 16 C.F.R. Part 313.3(k); 16 C.F.R. § 313.300(2) & (3).

The GLBA contains two parts. The Financial Privacy Rule requires financial institutions to provide their customers with a privacy notice and an accurate description of their current policies and practices with respect to protecting the confidentiality and security of the customer information. *See* 16 C.F.R. Part 313. The Safeguards Rule requires financial institutions to develop, implement, and maintain a comprehensive written information security program for protecting the security of the customer information and guarding against unauthorized disclosures. *See* 16 C.F.R. Part 314; The FTC's *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, *available at* <www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.shtm>. The FTC is the primary enforcer of the GLBA.

C. Additional Prominent Federal Privacy Laws

In addition to HIPAA and the GLBA, there are many other federal privacy laws that, although not regulating the acquisition and safekeeping of individual data, protect personal information. Several of these statutes include:

- The Federal Trade Commission Act (FTCA), 15 U.S.C. §§ 41–58. The FTCA applies to most companies and individuals doing business in the U.S., other than certain transportation, telecommunications, and financial companies (because these industries are primarily regulated by other federal agencies including but not limited to the Department of Transportation, the Commodity Futures Trading Commission and the Federal Communications Commission). This Act does not regulate categories of data, but is a federal consumer protection law that prohibits unfair or deceptive practices and, among other things, seeks monetary redress for conduct injurious to consumers.
- The Federal Trade Commission (FTC) has used its authority to charge companies that: (1) fail to protect consumer personal data, (2) have changed their privacy policies without adequate notice and an opportunity to opt out of the new privacy practice, and (3) fail to comply with a posted privacy policy. The FTC does not expressly require a company to have or disclose a privacy policy, but the FTC's position is that if a company discloses a privacy policy, it must comply with it.
- The Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510–2522, and the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. The ECPA and CFAA regulate the unauthorized interception, use, and disclosure of electronic communications and computer tampering, respectively. The ECPA applies to oral, wire, and electronic communications, including electronic and telephone communications. It applies to both the interception and the storage of oral, wire, and electronic communications and includes the Wiretap Act, the Stored Communications Act, and the Pen-Register Act. There are certain exceptions to this general standard under the ECPA. Examples of exceptions include:
  - a person, such as an employer, may intercept a wire, oral, or electronic communication where such person is a party to the communication, or
  - where one of the parties to the communication has given prior consent to such interception.

  See 18 U.S.C. § 2511(2)(a) & (d).

An employer's electronic communications policy will meet the consent exception if such policy informs employee they should have no expectation of privacy and the policy warns that the employer has the right to or will monitor file transfers, email messages, website usage, telephone communications, and the like.

The CFAA addresses the unauthorized access and use of computers and computer networks. The CFAA is primarily a criminal statute but it was amended in 1994 to allow individuals and companies to bring a private civil suit against a person who accessed a protected computer without authorization or while exceeding authorized access. Increasingly, employers are using the CFAA to bring suit against former employees or agents who have absconded with company data. See also the Stored Communications Act, 18 U.S.C. § 2701 *et seq*., which protects users whose electronic communications are in electronic storage with an electronic communications facility.

- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), 15 U.S.C. §§ 7701–7713 and 18 U.S.C. § 1037, and the Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227 *et seq*. The CAN-SPAM Act and the TCPA regulate the collection and use of email addresses and phone numbers, respectively. The CAN-SPAM Act specifically sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to demand that the sender cease sending email communication, and spells out tough penalties for violations. A "commercial message" is defined as an electronic message, the primary purpose of which is the commercial advertisement or promotion of a commercial product or service, including email that promotes content on commercial websites. *See* 15 U.S.C. § 7704(a). There is no exception for business-to-business email; all emails must comply with the law.

  The TCPA amended the Communications Act of 1934 and allows individuals to file lawsuits and collect damages for receiving unsolicited telemarketing calls, faxes, pre-recorded calls, or autodialed calls, among other forms of solicitation. The TCPA was recently amended, beginning on October 16, 2013, to eliminate the exception that advertisers could rely on an established business relationship (such as a previous purchase) to circumvent the need to obtain a consumer's written consent to receive telemarketing calls.

D. State Statutes on Internet Privacy

The latest trend in state statutes aims at protecting employees and students from being forced to disclose to an employer or an educational institution their user identification and passwords for social media and other Internet accounts. The following is a list of states that have passed laws protecting employees, students, or both from demands for such account information:

- Arkansas Act 998, Ark. Code Ann. § 6-60-104, Act 1480, Ark. Code Ann. § 11-2-124;
- California's Social Media Privacy Act, Cal. Lab. Code § 980; Cal. Educ. Code §§ 99120–99122;
- Colorado's Social Media Workplace Privacy Law, Colo. Rev. Stat. § 8-2-127;
- Delaware's Higher Education Privacy Act, Chapter 94, Del. Code Ann. § 9401 *et seq*.;
- Illinois' Right to Privacy in the Workplace Act, 820 Ill. Comp. Stat. § 55/1;
- Louisiana's Personal Online Account Privacy Protection Act, La. Rev. Stat. §§ 51:1951–51:1955;

- Maryland's Labor and Employment, User Name and Password Privacy Protection and Exclusions Act, MD. CODE ANN. § 3-712;
- Michigan's Internet Privacy Protection Act, MICH. PUB. ACT § 478;
- Nevada's Chapter 613 Employment Practices, Unlawful Acts of Employer Relating to Social Media Account of Employee or Prospective Employee, NEV. STAT. § 613.135;
- New Hampshire's Chapter 275 Protective Legislation, Use of Social Media and Electronic Mail, N.H. REV. STAT. ANN. § 275:74;
- New Jersey's Chapter 155, Prohibited Actions by Employers, N.J. STAT. ANN. § 34-6B-5 *et seq*.;
- New Mexico's Chapter 21, State and Private Education Institutions, Request for Access to Social Networking Account Prohibited, N.M. STAT. ANN. § 21-1-46;
- Oklahoma's Prohibited Actions Regarding Social Media Accounts-Exemptions-Civil Actions, OKLA. STAT. § 40-173.2;
- Oregon's Chapter 659A, Employers, Social Media Account Privacy, OR. REV. STAT. § 659A.330;
- Rhode Island's Student Social Media Privacy, R.I. GEN. LAWS §§ 16-103-1 – 6, and Employee Social Media Privacy, R.I. GEN. LAWS §§ 28-56-1 – 6;
- Tennessee's Employee Online Privacy Act, TENN. CODE. ANN. § 50-1-1001 *et seq*.;
- Utah's Internet Employment Privacy Act, UTAH CODE ANN. §§ 34-48-101–34-48-301;
- Washington's Prohibited Practices, Personal Social Networking Accounts-Restrictions on Employer Access, WASH. REV. CODE § 44.44.200; and
- Wisconsin's Internet Privacy Protection, WIS. STAT. § 995.55.

It is expected that other states will adopt similar legislation. At the federal level, there is currently a new bill, the Social Networking Online Protection Act, H.R. 537, which proposes to protect internet privacy (e.g., to prevent employers and certain other entities from demanding that employees provide a user identification and passwords for personal accounts on social networking websites).

§ 13.8 CONCLUSION

It is now well accepted that a person has a right to privacy under both the common law and statute. The right to privacy is generally only deemed infringed based upon an intentional act. A person may, however, waive a right to object or expressly consent to having his or her privacy invaded. The First Amendment right to free speech generally trumps a right to privacy, so privacy claims may be defeated where the publication of private information is newsworthy based on a legitimate public interest.

With the rise of the Internet, Congress and state legislatures have enacted statutes and regulations which take into account the ease and breadth of disclosure risk due to electronic communications. These statutes focus on the protection of private information held by regulated entities. Business lawyers should be familiar with the statutes and regulations relating to the industry of their client so they can effectively address privacy issues in contracts, and properly advise their clients.