U.S. District Court

No. 2002-255

HELEN REMSBURG, ADMINISTRATRIX OF THE ESTATE OF

AMY LYNN BOYER

v.

DOCUSEARCH, INC., d/b/a DOCUSEARCH.COM & a.

Argued: November 14, 2002

Opinion Issued: February 18, 2003

Gottesman and Hollis, P.A., of Nashua (David A. Gottesman and Anna Barbara Hantz on the brief, and Mr. Gottesman orally), for the plaintiff.

Getman, Stacey, Tamposi, Schulthess & Steere, PA, of Bedford (Andrew R. Schulman and Dona Feeney on the brief, and Mr. Schulman orally), for defendants Docusearch Inc., Wing and a Prayer, Inc. and Daniel Cohn.

Law Office of Hess & Fraas, of Bow (Carol L. Hess on the brief), for defendant Kenneth Zeiss.

Sichenzia Ross Friedman & Ference, of New York, New York (Steven B. Ross on the brief), and Brennan Caron Lenehan & Iacopino, of Manchester (Michael J. Iacopino on the brief and orally), for defendant Michele Gambino.

Chris J. Hoofnagle & a., of Washington, D.C., by brief, for the Electronic Privacy Information Center, as amicus curiae.

Scott H. Harris, of Manchester, by brief, for the New Hampshire Trial Lawyers

Association, as amicus curiae.

John M. Healy and Jordan G. Ulery, appearing pursuant to Supreme Court Rule 33(2), by brief, for the New Hampshire League of Investigators, Inc., as amicus curiae.

DALIANIS, J. Pursuant to Supreme Court Rule 34, the United States District Court for the District of New Hampshire (Barbadoro, C.J.) certified to us the following questions of law:

1. Under the common law of New Hampshire and in light of the undisputed facts presented by this case, does a private investigator or information broker who sells information to a client pertaining to a third party have a cognizable legal duty to that third party with respect to the sale of the information?

2. If a private investigator or information broker obtains a person's social security number from a credit reporting agency as a part of a credit header without the person's knowledge or permission and sells the social security number to a client, does the individual whose social security number was sold have a cause of action for intrusion upon her seclusion against the private investigator or information broker for damages caused by the sale of the information?

3. When a private investigator or information broker obtains a person's work address by means of a pretextual telephone call and sells the work address to a client, does the individual whose work address was deceitfully obtained have a cause of action for intrusion upon her seclusion against the private investigator or information broker for damages caused by the sale of the information?

4. If a private investigator or information broker obtains a social security number from a credit reporting agency as a part of a credit header, or a work address by means of a pretextual telephone call, and then sells the information, does the individual whose social security number or work address was sold have a cause of action for commercial appropriation against the private investigator or information broker for damages caused by the sale of the information?

5. If a private investigator or information broker obtains a person's work address by means of a pretextual telephone call, and then sells the information, is the private investigator or information broker liable under

N.H. Rev. Stat. Ann. § 358-A to the person it deceived for damages caused by the sale of the information?

For the reasons expressed below, we respond to the first, second and fifth questions in the affirmative, and the third and fourth questions in the negative.

I. Facts

We adopt the district court's recitation of the facts. Docusearch, Inc. and Wing and a Prayer, Inc. (WAAP) jointly own and operate an Internet-based investigation and information service known as Docusearch.com. Daniel Cohn and Kenneth Zeiss each own 50% of each company's stock. Cohn serves as president of both companies and Zeiss serves as a director of WAAP. Cohn is licensed as a private investigator by both the State of Florida and Palm Beach County, Florida.

On July 29, 1999, New Hampshire resident Liam Youens contacted Docusearch through its Internet website and requested the date of birth for Amy Lynn Boyer, another New Hampshire resident. Youens provided Docusearch his name, New Hampshire address, and a contact telephone number. He paid the $20 fee by
credit card. Zeiss placed a telephone call to Youens in New Hampshire on the same day. Zeiss cannot recall the reason for the phone call, but speculates that it was to verify the order. The next day, July 30, 1999, Docusearch provided Youens with the birth dates for several Amy Boyers, but none was for the Amy Boyer sought by Youens. In response, Youens e-mailed Docusearch inquiring whether it would be possible to get better results using Boyer's home address, which he provided. Youens gave Docusearch a different contact phone number.

Later that same day, Youens again contacted Docusearch and placed an order for Boyer's social security number (SSN), paying the $45 fee by credit card. On August 2, 1999, Docusearch obtained Boyer's social security number from a credit reporting agency as a part of a "credit header" and provided it to Youens. A "credit header" is typically provided at the top of a credit report and includes a person's name, address and social security number. The next day, Youens placed an order with Docusearch for Boyer's employment information, paying the $109 fee by credit card, and giving Docusearch the same phone number he had provided originally. Docusearch phone records indicate that Zeiss placed a phone call to Youens on August 6, 1999. The phone number used was the one Youens had provided with his follow-up inquiry regarding Boyer's birth date. The phone call lasted for less than one minute,

and no record exists concerning its topic or whether Zeiss was able to speak with Youens. On August 20, 1999, having received no response to his latest request, Youens placed a second request for Boyer's employment information, again paying the $109 fee by credit card. On September 1, 1999, Docusearch refunded Youens' first payment of $109 because its efforts to fulfill his first request for Boyer's employment information had failed.

With his second request for Boyer's employment information pending, Youens placed yet another order for information with Docusearch on September 6, 1999. This time, he requested a "locate by social security number" search for Boyer. Youens paid the $30 fee by credit card, and received the results of the search - Boyer's home address - on September 7, 1999.

On September 8, 1999, Docusearch informed Youens of Boyer's employment address. Docusearch acquired this address through a subcontractor, Michele Gambino, who had obtained the information by placing a "pretext" telephone call to Boyer in New Hampshire. Gambino lied about who she was and the purpose of her call in order to convince Boyer to reveal her employment information. Gambino had no contact with Youens, nor did she know why Youens was requesting the information.

On October 15, 1999, Youens drove to Boyer's workplace and fatally shot her as she left work. Youens then shot and killed himself. A subsequent police investigation revealed that Youens kept firearms and ammunition in his bedroom, and maintained a website containing references to stalking and killing Boyer as well as other information and statements related to violence and killing. II. Question 1

All persons have a duty to exercise reasonable care not to subject others to an unreasonable risk of harm. See Walls v. Oxford Management Co., 137 N.H. 653, 656 (1993). Whether a defendant's conduct creates a risk of harm to others sufficiently foreseeable to charge the defendant with a duty to avoid such conduct is a question of law, Iannelli v. Burger King Corp., 145 N.H. 190, 193 (2000), because "the existence of a duty does not arise solely from the relationship between the parties, but also from the need for protection against reasonably foreseeable harm." Hungerford v. Jones, 143 N.H. 208, 211 (1998) (quotation omitted). Thus, in some cases, a party's actions give rise to a duty. Walls, 137 N.H. at 656. Parties owe a duty to those third parties foreseeably endangered by their conduct with respect to those risks whose likelihood and magnitude make the conduct unreasonably dangerous. Hungerford,
143 N.H. at 211.

In situations in which the harm is caused by criminal misconduct, however, determining whether a duty exists is complicated by the competing rule "that a private citizen has no general duty to protect others from the criminal attacks of third parties." Dupont v. Aavid Thermal Technologies, 147 N.H. 706, 709 (2002). This rule is grounded in the fundamental unfairness of holding private citizens responsible for the unanticipated criminal acts of third parties, because "[u]nder all ordinary and normal circumstances, in the absence of any reason to expect the contrary, the actor may reasonably proceed upon the assumption that others will obey the law." Walls, 137 N.H. at 657-58 (quotation omitted).

In certain limited circumstances, however, we have recognized that there are exceptions to the general rule where a duty to exercise reasonable care will arise. See Dupont, 147 N.H. at 709. We have held that such a duty may arise because: (1) a special relationship exists; (2) special circumstances exist; or (3) the duty has been voluntarily assumed. Id. The special circumstances exception includes situations where there is "an especial temptation and opportunity for criminal misconduct brought about by the defendant." Walls, 137 N.H. at 658 (quotation omitted). This exception follows from the rule that a party who realizes or should realize that his conduct has created a condition which involves an unreasonable risk of harm to another has a duty to exercise reasonable care to prevent the risk from occurring. Id. The exact occurrence or precise injuries need not have been foreseeable. Iannelli, 145 N.H. at 194. Rather, where the defendant's conduct has created an unreasonable risk of criminal misconduct, a duty is owed to those foreseeably endangered. See id.

Thus, if a private investigator or information broker's (hereinafter "investigator" collectively) disclosure of information to a client creates a foreseeable risk of criminal misconduct against the third person whose information was disclosed, the investigator owes a duty to exercise reasonable care not to subject the third person to an unreasonable risk of harm. In determining whether the risk of criminal misconduct is foreseeable to an investigator, we examine two risks of information disclosure implicated by this case: stalking and identity theft.

It is undisputed that stalkers, in seeking to locate and track a victim, sometimes use an investigator to obtain personal information about the victims. See Note, Stalking Humans: Is There A Need For Federalization Of Anti-Stalking Laws In Order To Prevent Recidivism In Stalking?, 50 Syracuse L. Rev. 1067, 1075 (2000) (discussing two high profile California cases where the stalkers used investigators to obtain their victims' home addresses).

Public concern about stalking has compelled all fifty States to pass some

form of legislation criminalizing stalking. Approximately one million women and 371,000 men are stalked annually in the United States. P. Tjaden & N. Thoennes, Nat'l Inst. of Justice Ctr. for Disease Control and Prevention, Stalking in America: Findings from the National Violence Against Women Survey, Apr. 1998, at 2. Stalking is a crime that causes serious psychological harm to the victims, and often results in the victim experiencing post-traumatic stress disorder, anxiety, sleeplessness, and sometimes, suicidal ideations. See Mullen & Pathe, Stalking, 29 Crime & Just. 273, 296-97 (2002). Not only is stalking itself a crime, but it can lead to more violent crimes, including assault, rape or homicide. See, e.g., Brunner v. State, 683 So. 2d 1129, 1130 (Fla. Dist. Ct. App. 1996); People v. Sowewimo, 657 N.E.2d 1047, 1049 (Ill. App. Ct. 1995); Com. v. Cruz, 675 N.E.2d 764, 765 (Mass. 1997).

Identity theft, i.e., the use of one person's identity by another, is an increasingly common risk associated with the disclosure of personal information, such as a SSN. Komuves, We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers, 16 J. Marshall J. Computer & Info. L. 529, 534 (1998). A person's SSN has attained the status of a quasi-universal personal identification number. Id. at 531-32. At the same time, however, a person's privacy interest in his or her SSN is recognized by state and federal statutes, including RSA 260:14, IV-a (Supp. 2002) which prohibits the release of SSNs contained within drivers' license records. See also Financial Services Modernization Act of 1999, 15 U.S.C. §§ 6801-6809 (2000); Privacy Act of 1974, 5 U.S.C. § 552a (2000). "[A]rmed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits or Social Security benefits, order new checks at a new address on that person's checking account, obtain credit cards, or even obtain the person's paycheck." Greidinger v. Davis, 988 F.2d 1344, 1353 (4th Cir. 1993).

Like the consequences of stalking, the consequences of identity theft can be severe. The best estimates place the number of victims in excess of 100,000 per year and the dollar loss in excess of $2 billion per year. LoPucki, Human Identification Theory and the Identity Theft Problem, 80 Tex. L. Rev. 89, 89 (2001). Victims of identity theft risk the destruction of their good credit histories. This often destroys a victim's ability to obtain credit from any source and may, in some cases, render the victim unemployable or even cause the victim to be incarcerated. Id. at 91.

The threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client. And we so hold. This is especially true when, as in this case, the investigator does not know the client or the

client's purpose in seeking the information.

III. Questions 2 and 3

A tort action based upon an intrusion upon seclusion must relate to something secret, secluded or private pertaining to the plaintiff. Fischer v. Hooper, 143 N.H. 585, 590 (1999). Moreover, liability exists only if the defendant's conduct was such that the defendant should have realized that it would be offensive to persons of ordinary sensibilities. Id. "It is only where the intrusion has gone beyond the limits of decency that liability accrues." Hamberger v. Eastman, 106 N.H. 107, 111 (1964) (quotation omitted); see Restatement (Second) of Torts § 652B comment d at 380 (1977).

In addressing whether a person's SSN is something secret, secluded or private, we must determine whether a person has a reasonable expectation of privacy in the number. See Fischer, 143 N.H. at 589-90. SSNs are available in a wide variety of contexts. Bodah v. Lakeville Motor Express Inc., 649 N.W.2d 859, 863 (Minn. Ct. App. 2002). SSNs are used to identify people to track social security benefits, as well as when taxes and credit applications are filed. See Greidinger, 988 F.2d at 1352-53. In fact, "the widespread use of SSNs as universal identifiers in the public and private sectors is one of the most serious manifestations of privacy concerns in the Nation." Id. at 1353 (quotation omitted). As noted above, a person's interest in maintaining the privacy of his or her SSN has been recognized by numerous federal and state statutes. As a result, the entities to which this information is disclosed and their employees are bound by legal, and, perhaps, contractual constraints to hold SSNs in confidence to ensure that they remain private. See Bodah, 649 N.W.2d at 863.

Thus, while a SSN must be disclosed in certain circumstances, a person may reasonably expect that the number will remain private. Whether the intrusion would be offensive to persons of ordinary sensibilities is ordinarily a question for the fact-finder and only becomes a question of law if reasonable persons can draw only one conclusion from the evidence. See Swarthout v. Mutual Service Life Ins. Co., 632 N.W.2d 741, 745 (Minn. Ct. App. 2001). The evidence underlying the certified question is insufficient to draw any such conclusion here, and we therefore must leave this question to the fact-finder. In making this determination, the fact-finder should consider "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 expectations of those whose privacy is invaded." Bauer v. Ford Motor Credit Co., 149 F. Supp. 2d 1106, 1109 (D. Minn. 2001). Accordingly, a person whose SSN is obtained by an investigator from a credit reporting agency without the person's knowledge or permission

may have a cause of action for intrusion upon seclusion for damages caused by the sale of the SSN, but must prove that the intrusion was such that it would have been offensive to a person of ordinary sensibilities.

We next address whether a person has a cause of action for intrusion upon seclusion where an investigator obtains the person's work address by using a pretextual phone call. We must first establish whether a work address is something secret, secluded or private about the plaintiff. See Fischer, 143 N.H. at 590.

In most cases, a person works in a public place. "On the public street, or in any other public place, [a person] has no legal right to be alone." W. Page Keeton et al., Prosser and Keeton on the Law of Torts § 117, at 855 (5th ed. 1984).

A person's employment, where he lives, and where he works are exposures which
we all must suffer. We have no reasonable expectation of privacy as to our identity or as to where we live or work. Our commuting to and from where we live and work is not done clandestinely and each place provides a facet of our total identity. Webb v. City of Shreveport, 371 So. 2d 316, 319 (La. Ct. App. 1979). Thus, where a person's work address is readily observable by members of the public, the address cannot be private and no intrusion upon seclusion action can be maintained.

IV. Question 4

"One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy." Restatement (Second) of Torts § 652C at 380. In Hamberger, we noted that the law of invasion of privacy consists of four separate causes of action, including appropriation. Hamberger, 106 N.H. at 110-11. However, we have not had occasion to recognize appropriation as a cause of action within the State. We now hold that New Hampshire recognizes the tort of invasion of privacy by appropriation of an individual's name or likeness, and adopt the Restatement view. "The interest protected by the rule . . . is the interest of the individual in the exclusive use of his own identity, in so far as it is represented by his name or likeness, and in so far as the use may be of benefit to him or to others." Restatement (Second) of Torts § 652C comment a at 381.

Tortious liability for appropriation of a name or likeness is intended to

protect the value of an individual's notoriety or skill. Thus, the Restatement notes, in order that there may be liability under the rule stated in this Section, the defendant must have appropriated to his own use or benefit the reputation, prestige, social or commercial standing, public interest or other values of the plaintiff's name or likeness. The misappropriation tort does not protect one's name per se; rather it protects the value associated with that name. Matthews v. Wozencraft, 15 F.3d 432, 437 (5th Cir. 1994) (citation, brackets and quotation omitted). Appropriation is not actionable if the person's name or likeness is published for "purposes other than taking advantage of [the person's] reputation, prestige or other value" associated with the person. Restatement (Second) of Torts § 652C comment d at 382-83. Thus, appropriation occurs most often when the person's name or likeness is used to advertise the defendant's product or when the defendant impersonates the person for gain. Matthews, 15 F.3d at 437; see Restatement (Second) of Torts § 652C comment b at 381.

An investigator who sells personal information sells the information for the value of the information itself, not to take advantage of the person's reputation or prestige. The investigator does not capitalize upon the goodwill value associated with the information but rather upon the client's willingness to pay for the information. In other words, the benefit derived from the sale in no way relates to the social or commercial standing of the person whose information is sold. Thus, a person whose personal information is sold does not have a cause of action for appropriation against the investigator who sold the information.

V. Question 5

The last issue relates to the construction of the Consumer Protection Act, RSA chapter 358-A. "On questions of statutory interpretation, this court is the final arbiter of the intent of the legislature as expressed in the words of a statute considered as a whole." Franklin Lodge of Elks v. Marcoux, 147 N.H. 95, 96 (2001) (quotation omitted). We begin by considering the plain meaning of the words of the statute. Snow v. American Morgan Horse Assoc., 141 N.H. 467, 471 (1996). In conducting our analysis "we will focus on the statute as a whole, not on isolated words or phrases." Id. "[W]e will not consider what the legislature might have said or add words that the legislature did not include." Minuteman, LLC v. Microsoft Corp., 147 N.H. 634, 636 (2002) (quotation omitted).

RSA 358-A:2 (1995) states, in pertinent part: It shall be unlawful for any person to use . . . any unfair or deceptive act or practice in the conduct of any trade or commerce within this state. Such . . . unfair or deceptive act or practice shall include, but is not limited to, the following:

. . .

III. Causing likelihood of confusion or of misunderstanding as to affiliation, connection or association with . . . another.

Pretext phone calling has been described as the use of deception and trickery to obtain a person's private information for resale to others. See Com. v. Source One Associates, Inc., 763 N.E.2d 42, 47-48 n.8 (Mass. 2002). The target of the phone call is deceived into believing that the caller is affiliated with a reliable entity who has a legitimate purpose in requesting the information. RSA 358-A:2, III explicitly prohibits this conduct. The pretext clearly creates a misunderstanding as to the investigator's affiliation.

The defendant argues that our holding in Snow bars recovery in cases such as this because an investigator who makes a pretextual phone call to obtain information for sale does not conduct any "trade" or "commerce" with the person deceived by the phone call. The Consumer Protection Act defines "trade" and "commerce" as including "the advertising, offering for sale, sale, or distribution of any services and any property . . . ." RSA 358-A:1, II. There is no language in the Act that would restrict the definition of "trade" and "commerce" to that affecting the party deceived by the prohibited conduct. In fact, the Act explicitly includes "trade or commerce directly or indirectly affecting the people of this state." Id. (emphasis added). In Snow, we held that the registering of foals, alone, was not a transaction involving trade or commerce. Snow, 141 N.H. at 471. Such is not the case here. Here, the investigator used the pretext phone call to complete the sale of information to a client. Thus, the investigator's pretextual phone call occurred in the conduct of trade or commerce within the State.

The defendant argues that a person deceived by a pretextual phone call lacks standing to maintain a private cause of action under RSA chapter 358-A because only a buyer or seller in privity with the defendant may recover under the statute. We disagree. According to the statute, "[a]ny person injured by another's use of any method, act or practice declared unlawful under this chapter may bring an action for damages . . . ." RSA 358-A:10 (emphasis added). The statute defines who may bring a private action broadly, Milford Lumber Co. v. RCB Realty, 147 N.H. 15, 17 (2001), and by its plain meaning does not limit the class of persons who have standing to those in privity with the defendant.

We find support for this conclusion in the Massachusetts Consumer Protection Act, which is similar in many respects to the New Hampshire statute. See Milford Lumber Co., 147 N.H. at 18; see also Mass. Gen. Laws ch. 93A (1997). When the Massachusetts Consumer Protection Act was amended in 1979, section 9
was changed to permit "any person" (other than commercial entities covered under a separate section) to recover for damages, which "substantially broadened the class of persons who could maintain actions under [the statute]." Van Dyke v. St. Paul Fire and Marine Ins. Co., 448 N.E.2d 357, 360 (Mass. 1983). Consequently, Massachusetts courts have permitted third parties who were not in privity with the defendant to recover for damages caused by the defendant's violation of the statute. Maillet v. ATF-Davidson Co., Inc., 552 N.E.2d 95, 99 (Mass. 1990); see also Ellis v. Safety Ins. Co., 672 N.E.2d 979, 985-86 n.13 (Mass. App. Ct. 1996) (permitting the housemates of an insurance policyholder to maintain an action claiming racial harassment during an insurance investigation despite lack of privity).

Accordingly, we conclude that an investigator who obtains a person's work address by means of pretextual phone calling, and then sells the information, may be liable for damages under RSA chapter 358-A to the person deceived.

Remanded.

NADEAU and DUGGAN, JJ., concurred.