

OWNING THE RECORD – WHOSE E-DOCUMENT IS IT, ANYWAY?

*By Stephen M. Goodman**

Every successful business owner worries that the departure of a key employee may mean that critical business information is also walking out the door. Controlling confidential business information is part of building the value of a business, and losing control of that information can threaten that value.

In the past, when the information was only in paper form and making physical copies of documents was more challenging, it was easier for employers to keep the documents from being read by people outside the company. However, controlling the information has become much more difficult now that electronic media have become the primary means for creating and storing information and employers have made e-mail and electronic document systems available to all employees. Furthermore, employees have come to use these systems for personal activities as well as for the employer's business, making it more difficult to separate out documents and information which relate solely to the employer's business.

This general mixing of personal and business records has exacerbated conflicts regarding ownership of material such as client lists, where the information may be based on the employee's personal relationships, but is very valuable to the employer. While disputes about ownership of client lists pre-date the use of electronic document systems, recent cases involving use of those systems have resulted in decisions that may prove to be favorable to employers, provided that the employer makes clear to its employees that it is the owner of the system and that all material created using its system belongs to the employer.

Suppose, for instance, that you get a call from your client, Joe Smith, who is the president of Employment Services Incorporated (ESI), a New York corporation. He tells you that several weeks ago, ESI fired its long-time account manager, Robert Jones, because it suspected he was getting ready to jump ship to another firm. Robert began his employment with ESI straight from college, and during his years at ESI he built a substantial client base and generated millions of dollars in revenues for the firm. When ESI adopted company-wide e-mail and document storage systems, Robert loaded all of his contacts onto the system and conducted most of his correspondence electronically.

* *Stephen M. Goodman is a member of the Bar of the State of New York and a partner at the law firm of Pryor Cashman LLP. He acts as outside general counsel to publishing, media, computer software, pharmaceutical and biotechnology companies and other clients involved in the exploitation of intellectual property. The author wishes to thank his colleagues, Joshua Zuckerberg and Megan K. Gentile, for their assistance in preparing this article.*

Immediately upon Robert's termination, ESI locked Robert out of its computer system. Despite assertions in ESI's employee manual that ESI owns all material created and stored on its document system, Robert has demanded the opportunity to download a copy of his Outlook mailbox and contact list, as well as other memos and correspondence he had stored on the system. He claims that the stored material includes certain personal correspondence, including love letters to his girlfriend, Loretta.

Joe has refused Robert's repeated requests. Now Joe has received a demand letter from Robert's lawyer, threatening legal action if the material is not made available. Joe wants you to advise him what to do. Can he continue to refuse Joe any access to the stored material without any legal risk?¹

Companies such as ESI often include in their employee manuals and other employee communications notices such as the following: "All information and documents created, received, saved or sent on [the employer's] computer or communications systems are property of [the employer]."² There is logic inherent in the idea that if an employee is hired to work on employer premises, on employer time and using employer-provided resources, all information and documents generated by the employee in the course of his employment should belong to the employer.³ Based on the decision in at least one New York case, the fact that documents were created on the employer's document system may make irrelevant considerations as to whether the stored material constitutes a trade secret in determining whether the material is owned by the employer or the employee.

New York and most other jurisdictions award ownership to the employer if material created by an employee in the course of his employment satisfies the definition of a trade secret.⁴ In the frequently cited case of *Pullman Group, LLC v. Prudential Ins. Co., of America*, suit was brought by a company founded by Mr. Pullman, who, as a former employee of a brokerage firm, created a new form of complex financial transaction. When Pullman left his former employer, he asserted ownership of the trade se-

1. This is an issue which is distinct from an employer's monitoring of an employee's use of electronic systems in the course of his or her employment. *See, e.g.*, Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522, *cited in Fraser v. Nationwide Mutual Insurance Co.*, 352 F.3d 107 (3rd Cir. 2003).

2. *See, e.g.*, *Scott v. Beth Israel Med. Ctr. Inc.*, 17 Misc 3d 934, 942 (2007); *Garrity v. John Hancock Mutual Life Ins. Co.*, 2002 WL 974676, *1 (D Mass 2002); *In re Asia Global Crossing, Ltd.*, 322 B.R. 247 (S.D.N.Y. 2005).

3. *Cf.* Copyright Act, 17 U.S.C. § 101 (1976) (Employer is the "author" or an original work if it is a "work made for hire" defined as "a work prepared by an employee within the scope of his or her employment . . ."). *See also Shmueli v. Corcoran Group*, 802 N.Y.S.2d 871 fn. 5 (N.Y. Sup. Ct. 2005) (" . . . it is generally held that an employee's work product is proprietary to the employer," citing *Pullman Group, LLC v Prudential Ins. Co.*, 288 A.D.2d 2, 733 N.Y.S.2d 1 (1st Dept., 2001), *cert denied* 98 N.Y.2d 602 (2002)).

4. *See Pullman Group, LLC v. Prudential Ins. Co., of America*, 733 N.Y.S.2d 1 (App. Div. 2001), *citing Standard Parts Co. v. Peck*, 264 U.S. 52, 59 (1924).

cret represented by the features of the transaction, and sued to prevent the defendants from marketing the transaction.

The court accepted for purposes of reviewing the defendant's motion to dismiss that the material in question was a trade secret. However, it found that "the alleged trade secrets were created by Pullman while acting within the scope of his assigned duties as an employee of Gruntal and Fahnstock. . .and any such trade secrets were therefore owned by the employers *ab initio*."⁵

The *Pullman* court relied upon a United States Supreme Court case, *Standard Parts Co. v. Peck*, which reversed a Circuit Court of Appeals ruling and concurred with the original District Court determination that

. . . if [an employee] be employed to invent or devise . . . improvements, his patents therefor belong to his employer, since in making such improvements he is merely doing what he was hired to do."⁶ However, the District Court had come to this conclusion after (unhelpfully) stating that "the mere fact that one is employed by another does not preclude him from making improvements in the machines with which he is connected, and obtaining patents therefor, as his individual property"⁷

The *Pullman* case thus leaves employers with the challenge of having to show that the development of a particular trade secret or invention was the intended purpose of employment activities (in which case it would belong to the employer) rather than "merely incidental" to those activities (in which case it would belong to the employee).

The language generally used by the courts to distinguish between a trade secret and other types of (presumably unprotectible) information is also of limited utility. For example, in *A & G Research, Inc. v GC Metrics, Inc.*,⁸ the court stated, "Information that is ascertainable from outside sources or generally known in the trade cannot be misappropriated because it is not a proprietary trade secret. A trade secret is generally understood to be 'any formula, pattern, device or compilation of information utilized in one's business, and which provides an advantage over competitors who do not know or use it.'"⁹

On the one hand, this language (which is found in § 757, comment b, of the Restatement (First) of Torts) is broad enough to cover almost

5. *Pullman Group v. Prudential Ins. Co. of America*, 733 N.Y.S.2d 1, 3 (App. Div. 2001).

6. *Standard Parts Co. v. Peck*, 264 U.S. 52, 58 (1924).

7. *Id.*

8. 19 Misc 3d 1136 at *27 (N.Y. Sup. Ct. 2008) (*quoting* Restatement (First) of Torts, § 757 (1939), comment b.).

9. Note that the Uniform Trade Secrets Act defines "trade secret" as "information, including a formula, pattern, compilation, program device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." However, New York has not adopted the UTSA (Unif. Trade Secrets Act § 1(4) (amended 1985)).

any internal communication or other records of an employer. On the other hand, the courts have required that client lists meet certain additional requirements before determining that a particular list constitutes a trade secret. As a result, ownership of client lists, usually regarded by employers as “confidential information” critical to the employer’s business, is frequently challenged by employees seeking use of those lists for their own purposes.¹⁰

At least one New York case seems to offer a way to avoid the “trade secret” issue where a particular list has been created or stored on an employer-provided electronic document system. In *Scott v. Beth Israel Med. Ctr. Inc.*,¹¹ the defendant hospital refused to turn over certain correspondence between the plaintiff and the plaintiff’s attorney regarding a separate dispute. Scott filed a motion for a protective order seeking the return of the documents on the grounds that the correspondence was privileged under attorney-client privilege. According to the court, the hospital had clearly communicated in its policies that all documents created on its electronic systems were the property of the hospital and that employees had no personal privacy right in any material so created. Because Scott was on notice regarding these policies, the court held that Scott could not have made the communications in confidence.

Since preservation of the privilege depended on maintaining the confidentiality of communication, the court held that the correspondence was not privileged and, therefore, that the hospital did not have to return it. Significantly, however, the court in *Scott* allowed the hospital to retain the correspondence despite the fact that it could only be characterized as personal to the plaintiff and not useful to the defendant’s business – in other words, correspondence which was neither a trade secret nor even arguably confidential business information.

Although not a US case, the 2007 British decision in *PennWell Publishing (UK) Limited v. Ornstein et al.*¹² offers another variation on the issues raised in *Scott*. PennWell was in the business of publishing information and mounting conferences in the energy and power industries. The employee, Mr. Isles, worked for PennWell both as a journalist and a conference organizer. While he was employed, he created and kept all his contacts on his employer’s computer system, including both personal contacts and business contacts which he had prior to joining PennWell.

Mr. Isles’s employment contract stated that all documents used during his employment belonged to the company and had to be returned on termination. In addition, its e-mail policy stated that “Employees may

10. Compare *Kadant, Inc. v. Seeley Machine, Inc.*, 244 F. Supp. 2d 19 (N.D.N.Y. 2003) and *WMW Machinery Company, Inc. v. Koerber AG*, 658 N.Y.S.2d 385, 387 (2d Dep’t 1997) with *Repair Tech Inc. v. Zakarin*, 2005 WL 1845659 * 5 (N.Y. Sup. Ct. Kings County 2005) and *DoubleClick, Inc. v. Henderson*, 1997 WL 731413 (N.Y. Co. Ct. Nov. 7, 1997).

11. 17 Misc 3d 934 (2007).

12. *PennWell Publishing (UK) Limited v. Ornstein et al.* (2007) EWHC 1570 (QB) available at: <http://www.bailii.org/ew/cases/EWHC/QB/2007/1570.html>.

only use the e-mail system for business use.”¹³ Despite these policies, after Mr. Isles left PennWell and set up a competing business, the company discovered that he had downloaded his entire Outlook contacts list from his work laptop. PennWell applied for an injunction for return of the contacts list. Isles argued that most of the contacts on the list were personal to him and represented journalistic contacts necessary for his career.

The court held that where an address list is contained in Outlook or similar software that is part of the employer’s e-mail system and backed-up by the employer, the database or list belongs to the employer and may not be copied or removed in its entirety by employees for use outside or after employment. However, consistent with trade secret jurisprudence (though not finding the list to be a trade secret), the court indicated that such ownership could not be used by PennWell to prevent use by its former employee of “individual parts of its content which may be known to Mr. Isles by other means.”¹⁴

Because the employee in this case was a journalist, the court speculated that if Mr. Isles had created a separate file for personal contacts, and had demonstrated his use of some form of selection process to determine which contacts to place in this separate file, he could have retained the separate list or had access to it after termination.¹⁵ Unfortunately for Mr. Isles, because he had indiscriminately printed off the entire list of contacts built up during his employment, the court rejected his contention that the entire list was personal.

Two further points in *PennWell* merit discussion. First, the court in *PennWell* distinguished journalists from other types of employees, such as salesmen, saying that removal of contact details by salesmen would be detrimental to the employer, whereas journalists need to build up contacts for use in obtaining information for articles. So employees who cannot argue that control of their contact list impinges on “freedom of the press” may be unable to rely much on *PennWell*.

More significantly, in contrast to *Scott*, the court found that PennWell’s document policy had not been adequately communicated to Isles.¹⁶ Because of this failure, although finding that the contact list as a whole belonged to PennWell, the court allowed Mr. Isles to take copies of personal information, including contacts he had established prior to joining PennWell, and (in the case of truly confidential personal information, such as details of an employee’s doctor) to have the information deleted from PennWell’s system.¹⁷

From an employer’s standpoint, it is instructive to look for possible reasons for the different outcomes in *PennWell* and *Scott* regarding em-

13. *Id.*

14. *Id.*

15. *Id.*

16. *Id.*

17. *Id.*

ployee rights to personal information. The *PennWell* court allowed the employee the right to copy and in some instances to delete demonstrably personal information because his employer had failed to adequately communicate its e-mail policy to him. Possibly because Dr. Scott was expressly found to be on notice regarding the hospital's e-mail policy, the court in *Scott* did not feel compelled to give him access to his personal correspondence or to order the hospital to delete the correspondence from its system. Thus, clear communication of these policies appears to be imperative in order to maximize an employer's rights to electronic records, including correspondence.

Employers should be aware, however, that if an employee is able to demonstrate that material is purely personal, proper communication of document policies to employees may not save the employer from damage claims if they refuse to relinquish the material even if it has been created on the employer's system. At least where independent contractors are concerned, certain New York cases have allowed the individual to bring such claims.

In *Shmueli v. Corcoran Group*,¹⁸ Shmueli was a real estate agent who was engaged as an independent contractor and was provided by her employer, The Corcoran Group, with "an office equipped with essentials, such as a computer and a telephone."¹⁹ According to the complaint, over her five years with Corcoran, Shmueli maintained computer records of all deals from her fourteen-year career, including those which had been "prior to, and independent of, her association with" Corcoran.²⁰ She also maintained a hard copy list of approximately three hundred business contacts.²¹

Upon her termination, Corcoran immediately changed Shmueli's computer access code and removed her hard copy list of contacts from her office.²² Shmueli then brought an action for damages alleging (among other things) conversion, breach of bailment and misappropriation of proprietary information.²³ Defendants moved for summary judgment dismissing the complaint.²⁴

The court accepted that the electronic list and the hardcopy list were both "property" and given the posture of the case as a motion for summary judgment, also accepted the allegations in Shmueli's complaint that the property was "owned" by her. Because there was no dispute as to Shmueli's status as an independent contractor, the court further accepted that the suppliers and equipment made available to Shmueli were

18. 802 N.Y.S.2d 871 (N.Y. Sup. Ct 2005).

19. *Id.* at 878.

20. *Id.* at 873.

21. *Id.*

22. *Id.*

23. *Id.*

24. *Id.*

furnished as “items licensed to her in facilitation of her independent contract with Corcoran.”²⁵

As a result, the court expressly refused to find that Corcoran owned the contact list simply because the list was stored in the system Corcoran had supplied to Shmueli. Since the court accepted that the lists were her property and that she was entitled to control access to her property even though stored in the “leased” equipment (whether a file cabinet for the hard copy or the computer files for the electronic records), the court found that Shmueli had shown the elements necessary for a claim of conversion and refused to dismiss her claim.²⁶ Giving the plaintiff’s assertions “every favorable inference” in deciding the summary judgment motion, the court also allowed additional claims for breach of bailment and misappropriation of proprietary information to proceed.²⁷

A similar analysis was applied by the United States Court of Appeals for the Second Circuit in *Thyroff v. Nationwide Mutual Insurance Company*.²⁸ As in *Shmueli*, Thyroff was an independent contractor, in this case engaged as an insurance agent by Nationwide. As part of his contract, Nationwide “required that Thyroff lease an agency office-automation system (AOA), including hardware and software, from Nationwide.”²⁹ According to the court, Thyroff’s office operations were “very much dependent” on the AOA.³⁰ Information which was uploaded by Nationwide nightly from Thyroff’s computers included not only business information but Thyroff’s personal information “unrelated to Nationwide’s business”.³¹

Again, as in *Shmueli*, when Thyroff was terminated, Nationwide denied Thyroff access to the AOA and, in this case, reclaimed its equipment. As a result, Nationwide took “various files — including personal e-mail, documents, and assorted data — that Thyroff stored on the system,” as well as data that Thyroff had compiled regarding Nationwide custom-

25. *Id.* at 876.

26. *Id.* The court expressly stated that its refusal to give Corcoran’s ownership of the computers any weight was based in part on Shmueli’s status as an independent contractor. “The within holdings are not intended to extend to cases involving employees (as opposed to independent contractors), as it is generally held that an employee’s work product is proprietary to the employer.” (citing *Pullman, supra.*). The case leaves open the possibility, however, that if for some reason the work product is found *not* to belong to the employer, refusal to make it available would bring the employee’s claims within the court’s reasoning in *Shmueli*.

27. *Id.* at 878. With regard to misappropriation claim, the court accepted the plaintiff’s assertion that her client list and transactional list were “proprietary, confidential information” compiled with “considerable time, effort, and cost,” in which case it seems to conclude that the lists amounted to protectible trade secrets.

28. *Thyroff v. Nationwide Mutual Ins. Co.*, 460 F.3d 400 (2d Cir. 2006).

29. *Id.* at 401.

30. *Id.*

31. *Id.*

ers “that Thyroff needed in order to retain his customer’s business once his relationship with Nationwide ended.”³²

Thyroff sued for, among other things, conversion of the personal information and programs he had stored on the AOA. The District Court initially dismissed Thyroff’s conversion claim, finding in part that the business records stored on the AOA could not be converted because Nationwide owned the AOA.³³ The Second Circuit disagreed, stating that “Nationwide owns the AOA, but that does not mean that it also owns any records that Thyroff may have saved on the system. . . . Had Nationwide leased Thyroff a filing cabinet into which Thyroff placed his personal property, such as a camera, Nationwide would not contend that it could seize Thyroff’s camera when it reclaimed its filing cabinet. The instant situation is no different. *This argument could be tenable if Thyroff had agreed to such terms*, but the AOA lease agreement contains no such language transferring the ownership of Thyroff’s personal property that he saved on the AOA to Nationwide.”³⁴ In addition, because it was not clear from the face of the agency agreement that Nationwide was the owner of policyholder information, the court insisted that, for purposes of the motion to dismiss, it was necessary to accept Thyroff’s allegation that the information belonged to him.³⁵

Although the courts in *Shmueli* and *Thyroff* allowed the plaintiffs to proceed with their claims of conversion, it is unclear that the result would have been the same if the individual had been an employee rather than an independent contractor. Assuming proper communication of detailed document ownership policies to employees, the question is whether the fact that the material in question is created on the employer’s system trumps any and every assertion of ownership by an employee, regardless of the nature of the content. In other words, if Thyroff had been an employee, would proper communication of Nationwide’s document policies to him give Nationwide rights equivalent to Thyroff’s “agreement” that Nationwide would be the owner of policyholder information compiled on its system?

Returning to Joe’s request for advice, you could advise him that, notwithstanding *Shmueli* and *Thyroff*, Robert’s ability to recover the retained records would face fairly substantial hurdles, particularly if ESI’s policy regarding employee use of its electronic systems has addressed all of the necessary property issues and ESI is able to show that it communicated

32. *Id.* at 408.

33. *Thyroff v. Nationwide Mutual Ins. Co.*, 2004 WL 2397614 (W.D.N.Y. 2004). Because the Second Circuit determined that New York had not yet recognized a claim for conversion of intangible electronic records and data (as opposed to tangible personal property), it certified the question to the New York Court of Appeals. In response, the Court of Appeals found that such records and data could be the subject of a claim for conversion. *Thyroff v. Nationwide Mutual Insurance Co.*, 8 N.Y.3d 283 (App. Div. 2007).

34. *Thyroff*, 460 F.3d at 410 (emphasis added).

35. *Id.*

this policy effectively to Robert. Under those circumstances, *Scott* seems to indicate that ESI has no obligation to turn over even personal material such as Robert's love letters if they were created by him using the company's system. Even if a New York court were willing to adopt the exceptions for separately maintained files and lists outlined in the *PennWell* case, Robert probably would not be able to rely on them since he cannot claim to be a journalist.

In short, if an employer properly communicates its document policies to its employees, *Scott* seems to remove any burden the employer might otherwise have to demonstrate that a particular record constitutes a trade secret in order to justify its retention. Instead, under that case and even under *PennWell*, proper communication of the policies seems to shift the burden onto the employee to demonstrate why the employer should relinquish control of any documents, even if they are personal to the employee. If this is a proper reading of those cases, then where the material arguably represents a mixture of personal and business information, such as client or customer lists, as opposed to purely personal information, both *Scott* and *PennWell* seem to strengthen the employer's ability to retain exclusive control of those lists, even if those lists cannot meet the requisite tests for a trade secret.