Washington Journal of Law, Technology & Arts

University of Washington School of Law

VOL. 6 SUMMER 2010 NO. 1

CONTENTS

Washington Journal of Law, Technology & Arts

University of Washington School of Law

VOL. 6 SUMMER 2010 NO. 1

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 6, ISSUE 1 SUMMER 2010

WALKING FROM CLOUD TO CLOUD: THE PORTABILITY ISSUE IN CLOUD COMPUTING

Robert H. Carpenter, Jr. [*]

CITE AS: 6 WASH. J.L. TECH. & ARTS 1 (2010)
https://digital.lib.washington.edu/dspace-law/handle/1773.1/447

ABSTRACT

Cloud computing has become popular among businesses that see information technology as outside their core competencies, demand a highly flexible computing environment, and seek to achieve more predictable costs. In some ways, cloud computing resembles IT outsourcing arrangements used in the financial services industry for many years; therefore lessons from financial services IT outsourcing agreements may prove helpful to parties interested in adopting cloud computing. This article considers the use of "data hostage" clauses in combination with arbitration or litigation clauses by service providers and the problems these clauses can cause outsourcing businesses. These two clauses together can insulate service providers from liability for material breaches and be used to coerce non-breaching customers into paying hefty termination fees. Although careful analysis shows that data hostage clauses may not always be enforceable, few customers are likely to litigate these cases. This Article considers regulatory and contract drafting strategies for reducing the risks to outsourcing businesses arising from the use of such clauses.

---

[*] Robert H. Carpenter, Jr. has a solo practice in Plano, Texas. Mr. Carpenter's practice focuses on mergers and acquisitions of and investment in small and closely held businesses and on information technology. His mergers and acquisitions and investment practice includes due diligence design and implementation, deal structuring, and contract negotiation. In the technology practice, he assists clients in negotiating and documenting information technology outsourcing contracts, license agreements and technology development arrangements. He also represents information technology clients in alternative dispute resolution.

TABLE OF CONTENTS

INTRODUCTION

Today information technology (IT) is exploring a new frontier: the cloud. Cloud computing is the enticing alternative to do-it-yourself, in-house information technology solutions.[1] In the cloud computing model, data is initially captured by the outsourcing business, transmitted to the service provider, processed by the service provider, stored within the service provider's computers, and then remotely accessed via a network. (In some cases, the data is partially and periodically downloaded to local servers at the outsourcing business for local viewing or customized reporting.)[2] Simply put, "plugging into the IT cloud . . . [is] browser access to an application hosted on the Web."[3]

---

[1] *See* Scott Morrison, *'Cloud Computing' Makes Gains*, WALL ST. J., Aug. 20, 2008, at B3B.

[2] J. Nicholas Hoover & Richard Martin, *Demystifying the Cloud*, INFO. WK., June 23, 2008, at 32, *available at* http://www.informationweek.com/news/services/hosted_apps/showArticle.jhtml?articleID=208700713 (noting that common characteristics of cloud computing include "IT resources provisioned outside of the corporate data center, those resources accessed over the Internet, and variable cost.").

[3] *Id.* at 30. The U.S. Government's more comprehensive working definition of "cloud computing" expands upon the simple definition:

> Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This

For instance, Amazon Web Services, a leader in cloud computing, now offers data storage and data processing and database management services—all via the Internet.[4] Rather than using on-premises software and systems and data storage, a user employs those of a vendor specializing in "cloud" services. The familiar "software as a service" (SaaS) is one of several service models for cloud computing.[5]

Critics of the cloud raise concerns over the portability of cloud computing because the cloud computing model requires that data reside with the service provider.[6] The outsourcing business experiences the negative impact of this lack of portability, or "vendor lock-in" phenomenon, when it wants to migrate to another cloud computing service provider and is confronted with a data hostage clause in its outsourcing agreement requiring the business to pay an applicable termination fee in order for the data to be returned.[7] This Article will examine the portability dilemma faced by outsourcing businesses and propose two possible strategies to resolve the portability dilemma for future outsourcing businesses.

I. THE PORTABILITY DILEMMA

For years, IT service providers have included a "data hostage" clause in their outsourcing contracts to discourage customer defections. Such data hostage clauses might include the following language:

> Customer consents and agrees and authorizes Service

> cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**.

Peter Mell & Tim Grance, Draft NIST Definition of Cloud Computing 1 (Oct. 7, 2009), http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc (emphasis in original).

[4] Hoover & Martin, *supra* note 2.

[5] *See* Mell & Grance, *supra* note 3.

[6] Bob Preston, *Customers Fire a Few Shots at Cloud Computing*, INFO. WK., Jun. 16, 2008, at 52, *available at* http://www.informationweek.com/news/services/data/showArticle.jhtml?articleID=208403766.

[7] *See Apple Says "Uncle,"* CARPENTER LAW OFFICE CLIENT NEWSLETTER (Robert H. Carpenter, Jr., Plano, Tex.), Jan. Feb. 2007, *available at* http://0093d40.netsolhost.com/images/Apple_Says_Uncle__Jan._-_Feb._2007__2007.pdf.

> Provider to retain Customer files until (i) Service Provider is paid in full for (A) all services provided through the date such Customer files are returned to Customer; and (B) any and all other amounts that are due or will become due under this Agreement; (ii) Service Provider is paid its then standard rates for the services necessary to return such Customer files; (iii) if ***this Agreement is being terminated, Service Provider is paid any applicable termination fee***; and (iv) Customer has returned to Service Provider all confidential and proprietary information received from Service Provider.

When a customer seeks to terminate an outsourcing agreement, the service provider typically denies that any material breach of contract has occurred or that a customer has any basis to terminate for cause, and demands payment in full or a large termination fee, representing liquidated damages for lost business. The service provider may simply hold the customer's data hostage until payment is made. To the extent that outsourcing businesses realize there is a risk of opportunistic behavior on the part of service providers, they will be less likely to adopt cloud computing; to the extent that outsourcing businesses do not recognize the risks up front, outsourcing IT with services such as cloud computing creates traps for the unwary.

One possible strategy to mitigate this risk, currently used by the financial industry, is for the outsourcing business to seek shorter service contract durations. In the past, financial institutions and their IT service providers have committed to long-term outsourcing relationships ranging from five to even ten-year terms. More recently it has become uncommon for service contract terms to exceed five years; and some are as short as three years. Even renewal terms in current agreements are narrowing. Renewal terms were often the same as the initial term; now many are for a single year. Rapid developments in information technology resulted in Federal bank regulators to issue this cautionary note:

> [C]ontracts need to be flexible, and therefore, should not be long-term (over five years). It is difficult to foresee and contract for every possible contingency that

> may arise. Also, business needs change or the market may evolve in unexpected directions. For these reasons, OTS discourages long-term contracts. Shorter contracts may provide more flexibility to meet the challenges of a changing environment.[8]

Anecdotal evidence suggests that some cloud computing providers, probably sensitive to the data portability issue and the barrier it erects to business migration to the cloud computing model, have shortened required contract terms or even eliminated them altogether. Such concessions are, however, unlikely when there are substantial front-end costs; parties will therefore likely continue to engage in high-stakes disputes.[9]

II. CASE STUDY

Because there are no reported decisions that offer a clear solution to the data portability dilemma, anecdotal evidence of an actual dispute may be a helpful guide for analysis. The following case study is based on an actual dispute that settled before going to trial. While the names are fictional, the parties represent real players in the financial services IT outsourcing space.

In 2007, when Happy Valley Bancshares renewed its IT outsourcing contract with Nifty Data Processing for a second five-year

---

[8] OFFICE OF THRIFT SUPERVISION, THRIFT BULLETIN 82A, THIRD PARTY ARRANGEMENTS 15 (2004), *available at* http://www.ots.treas.gov/_files/84272.pdf. This bulletin, like its 2003 predecessor, mandates (at least for the thrifts that OTS regulates) a shortening of contract terms, a process that had already begun taking place through outsourcing by U.S. financial institutions of back office business.

[9] The author's experience in this field spans the last decade. As legal counsel for IT service providers, he has prosecuted the collection of liquidated damages in over ten such disputes, many involving more than a million dollars claimed against a serviced business. In every case except two, the serviced business conceded payment of liquidated damages in order to secure its data. In the two exceptions, the serviced business filed preemptive actions in state courts that ultimately forced the service provider to relent rather than suffer negative publicity. Alltel Info. Svcs., Inc. v. Fed. Deposit Ins. Corp., 194 F.3d 1036 (9th Cir. 1999), is the only reported decision addressing termination of an IT services outsourcing contract and payment of liquidated damages for the termination. The Alltel claim for $1.4 million demonstrates the high-stakes nature of such disputes.

term, Nifty agreed to improve its service to remain competitive. There were four significant provisions included in the IT outsourcing contract: (1) Happy Valley retains ownership of the data after transmittal to Nifty and Nifty acknowledges that such data is Happy Valley's exclusive property; (2) Nifty accepts possession of the data subject to the agreed upon restrictions on use; (3) any claim arising from the agreement is subject to arbitration; and (4) data is subject to a hostage clause.[10]

When Nifty failed to meet the newly negotiated service level agreements because, unlike its competitors, it was unable to meet emerging performance standards, Happy Valley claimed that Nifty had materially breached the new IT outsourcing contract.[11] Happy Valley entered into negotiations with a different IT vendor and demanded that Nifty surrender Happy Valley's customer data in its most portable or native format[12] so the change in vendors could proceed. Nifty denied any contract breach and refused to turn over any of its data unless Happy Valley paid four million dollars in liquidated damages for contract termination.[13] Analysis of the outsourcing relationship

---

[10] Provisions such as "Nifty further acknowledges and agrees that all confidential data described in this Agreement is and constitutes information that belongs wholly to and is the exclusive property of Happy Valley" and "Confidential data will at no time be used by Nifty directly or indirectly other than as necessary to carry out its obligations under and for purposes authorized in this Agreement" are typical for financial institution IT services outsourcing contracts. *See* FED. FIN. INST. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK, OUTSOURCING TECHNOLOGY SERVICES BOOKLET 13 (2004) [hereinafter OUTSOURCING TECHNOLOGY SERVICES], *available at* http://www.ffiec.gov/ffiecinfobase/booklets/outsourcing/Outsourcing_Booklet.pdf.

[11] Service level agreements (SLAs) are metrics prescribed in an IT services contract used to measure the service provider's performance. Depending upon the contract's terms, failure to meet an SLA may constitute a material breach of the contract, or it may simply give rise to a nonperformance monetary credit against the contract's service charges.

[12] PCMag.com Encyclopedia, http://www.pcmag.com/encyclopedia_term/02542,t=native+format&i=47655,00.asp (last visited Nov. 17, 2009) (defining native format as the most complete and portable data file format that a computer application reads and writes).

[13] Early contract terminations usually invoke liquidated damages clauses that require payment of all or a large portion of the payments that would have been made if the contract had continued. These payments are almost always a substantial sum.

and terms of the agreement suggests Happy Valley may have not only contract claims against Nifty, but also tort claims.

A. Tort Claims Arising from Contracts

A tort is "a breach of a duty that the law imposes on persons who stand in a particular relation to one another."[14] Happy Valley satisfies the three requirements for an action in tort by demonstrating: (1) the existence of Nifty's duty to Happy Valley, (2) Nifty's breach of that duty, and (3) damages proximately caused by the breach. Happy Valley claims the IT outsourcing contract created a bailment for hire in which Happy Valley entrusted its property to Nifty for specific and limited purposes and for which Happy Valley paid Nifty. Nifty, a bailee, rightfully came into possession of the property, but owed Happy Valley a duty to return the data upon demand.[15] Because Nifty breached its duty as a bailee by failing to return the property upon demand, Happy Valley was prevented from transferring to a new service provider and therefore suffered non-economic damages and incidental economic damages.

At common law, Happy Valley would have had a remedy against Nifty in either detinue or replevin for return of personal property that was lawfully obtained but wrongfully detained after Happy Valley's demand for its return.[16] Because section 78.01 of the Florida Statutes provides a remedy of replevin,[17] and the action of detinue is

---

[14] BLACK'S LAW DICTIONARY 1526 (8th ed. 2004).

[15] *See* So. Mill Creek Prod. Co. v. Ferrell Jewelers of Tampa, Inc., 194 So. 2d 690 (Fla. Dist. Ct. App. 1967); S. Indus. Sav. Bank v. Greene, 224 So. 2d 416, 418-19 (Fla. Dist. Ct. App. 1969), *cert. denied*, 232 So. 2d 181 (Fla. 1969) (noting that the compensated bailee, when compared to an involuntary or gratuitous bailee, owes the bailor the highest duty of care with respect to bailed property).

[16] Williams Mgmt. Enter., Inc. v. Buonauro, 489 So.2d 160, 161 n.1 (Fla. Dist. Ct. App. 1986).

[17] FLA. STAT. § 78.01 (2009). Florida breaks with the line of cases exemplified by S. Cent. Bell Telephone Co. v. Barthelemy, 643 So. 2d 1240 (La. 1994) (holding computer software recorded on disks, tapes, or hard drives have a physical form and are thus subject to tangible personal property tax) and instead decides that "the physical components of software—the same discs, tapes, hard drives, etc.—discussed by the Louisiana court, are only 'tangential incidents' of the program" and, thus, are not tangible personal property subject to taxation. Gilreath v. Gen. Elec. Co., 751 So. 2d

considered obsolete in Florida, Happy Valley chose to sue Nifty pursuant to the Florida replevin statute.[18]

The legal remedy of replevin arises out of a tort claim rather than a contract claim.[19] However, the *Restatement (Second) of Torts* suggests that either a tort claim or a contract claim may be appropriate: "an act and its consequences may be both a tort and a breach of contract. . . . When this is so, the injured person, although barred by a statute from maintaining an action of tort may not be barred from enforcing his contractual . . . right *or vice versa*."[20] Florida follows this rule, at least when the tort is independent from the underlying contract.[21] Therefore, Happy Valley may recover on a tort claim arising from a contractual relationship "if the defendant's conduct constituted a separate and independent tort."[22]

705, 709 (Fla. Dist. Ct. App. 2000). Nevertheless, in the replevin context, this analysis is not applied:

> [I]ntangible personal property must be clearly distinguished from tangible evidence of intangible property, which tangible evidence can usually be identified and, when it can be, such tangible evidence may be the subject of an action of replevin when the issue is who is entitled to the immediate possession of the physical object, but not when the issue is the ownership of the intangible right that is represented by the tangible evidence.

Williams Mgmt. Enter., 489 So. 2d at 163-64 (footnotes omitted). Because Happy Valley's ownership of the underlying customer was not in doubt, Happy Valley could have replevied physical objects containing the data.

[18] *See generally Williams Mgmt. Enter.*, 489 So.2d at 161 n.1 (noting that "[o]riginally detinue was purely an action to recover goods in specie, if obtainable, and if not, their value at the time of the verdict, in cases where there was no wrongful taking. . . . [Although] the action of detinue has never been formally abolished, it is usually said that the action of detinue is obsolete because in Florida, now by statute, replevin relates to property both wrongfully taken and wrongfully detained.").

[19] *Id.* at 161.

[20] RESTATEMENT (SECOND) OF TORTS § 899 cmt. b (1979) (emphasis added).

[21] HTP, Ltd. v. Lineas Aereas Costarricenses, S.A., 685 So. 2d 1238, 1239 (Fla. 1996) (stating that "[w]here a contract exists, a tort action will lie for either intentional or negligent acts considered to be independent from acts that breached the contract."). *Cf.* Samuels v. King Motor Co., 782 So.2d 489, 498 (Fla. Dist. Ct. App. 2001) (allowing alternative counts in contract and tort for claims arising from a contract of bailment).

[22] Michael Dorff, *Attaching Torts Claims to Contract Actions: An Economic Analysis of Contort*, 28 SETON HALL L. REV. 390, 406 (1997). *But see id.* at 408-10 (noting this

The "contort" dilemma, and the analysis of whether an action should be brought in contract or in tort, can also be explained this way:

> Ordinarily, a breach of contract is not a tort . . . . However, a contract may create a state of things which furnishes the occasion of a tort, so that the negligent performance of a contract may give rise to an action in tort, if the duty exists independently of the performance of the contract. The contract then creates the relation out of which grows the duty to use care in the performance of a responsibility prescribed by the contract.[23]

While this formulation seems much broader than, and possibly at odds with, Florida's rule, these approaches can be reconciled:

> There are, however, a few situations in which failure to perform a contract may amount to a tort . . . . [One] type of exception arises where the contract results in or accompanies some relation between the parties which the law recognizes as giving rise to a duty of affirmative care. The typical case is that of a bailment, where the bare fact that the defendant has possession of the

---

"straightforward" rule has spawned competing analytical frameworks).

[23] 57A AM. JUR. 2D *Negligence* § 110 (2004) (footnotes omitted). Much of the discussion of contorts, and whether a plaintiff who is in contractual privity with the defendant should be barred from maintaining a tort claim, centers on money damages and application of the economic loss rule, which "is designed to prevent parties to a contract from circumventing the allocation of losses set forth in the contract by bringing an action for economic loss in tort." Indemnity Ins. Co. of No. Am. v. Am. Aviation, Inc., 891 So. 2d 532, 536 (Fla. 2004). *See also* Amy G. Doehring, *Blurring the Distinction between Contract and Tort: Courts Permitting Business Plaintiffs to Recover Tort Damages for Breach of Contract*, 12 BUS. TORTS J. 2, 1 (2005), *available at* www.mwe.com/info/pubs/aba05.pdf. Because Happy Valley primarily asked for recovery of its property and only economic loss incidental to the wrongful restraint (damages specifically allowed by Florida's statutory replevin action) the economic loss rule has no application in the analysis of the viability of Happy Valley's tort claim. FLA. STAT. § 78.01 (2009) (stating that "[a] person whose personal property is wrongfully detained . . . may . . . recover . . . any damages sustained by reason of the wrongful . . . detention").

> plaintiff's property is enough to create the duty, and it would exist if there were no contract at all and the goods were found on the highway.[24]

Nifty, the bailee for hire—a situation based upon the contract between the parties—owed a duty to Happy Valley, the bailor, to use due care in holding bailor's property and to return it upon demand.[25] When Nifty failed to return the property and proximately caused damages to Happy Valley, Happy Valley was able to bring a tort claim against Nifty for replevin under section 78.01 of Florida Statutes. While Happy Valley may theoretically bring this tort claim against Nifty, the data hostage and arbitration clauses in the IT outsourcing contract data hostage clause attempt to interpose a contractual bar to Happy Valley's suit.

B. Exculpatory Contract Provisions

The data hostage clause requires Happy Valley to pay Nifty a termination fee when terminating without cause. The self-help remedy provided by the data hostage clause allows the service provider to make the initial determination whether it has breached the contract. While subsequent litigation or arbitration might result in a victory for the outsourcing business, the aggrieved customer may be unable to leave its data in possession of the service provider long enough to achieve victory.

IT services outsourcing agreements typically include arbitration clauses or litigation provisions governing choice of law and forum. Happy Valley's contract with Nifty included an arbitration clause: "any controversy or claim arising out of or relating to this Agreement, or the breach thereof, shall be settled by arbitration." In recognition of this provision, Happy Valley filed a demand for arbitration claiming that Nifty had materially breached the IT outsourcing contract. The demand for arbitration claimed money damages caused by Nifty's breaches and requested an award of specific performance of Nifty's

---

[24] W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS 662-63 (5th ed. 1984) (footnotes omitted). *See also* DAN B. DOBBS, THE LAW OF TORTS 5 (2000).

[25] *See* So. Mill Creek Prod. Co., 194 So. 2d 690.

obligation to return Happy Valley's data so that the conversion to a new service provider could take place. The arbitration, however, proceeded very slowly.

The data hostage and arbitration clauses together may give a breaching service provider the leverage to coerce an outsourcing business to pay a termination fee to which it is not entitled. To proceed with the tort claim in court, Happy Valley must demonstrate that the clauses taken together constitute exculpatory clauses and are thus unenforceable. *Restatement (Second) of Contracts* states exculpatory contract clauses are unenforceable when "[a] term exempting a party from tort liability for harm caused intentionally or recklessly is unenforceable on grounds of public policy."[26]

In Florida exculpatory contract clauses may be enforceable, but:

> As frequently recognized by the Florida courts, exculpatory clauses [not only for negligent, but also for willful, malicious or grossly negligent actions] are not favored in the law, and Florida law requires that such clauses be strictly construed against the party claiming to be relieved of liability. Such clauses are enforceable only where and to the extent that the intention to be relieved was made clear and unequivocal in the contract, and the wording must be so clear and understandable that an ordinary and knowledgeable party will know what he is contracting away.[27]

In *O'Connell v. Walt Disney World Co.* the court discusses an exculpatory contract clause in contrast to an indemnification or an assumption of risk clause. In the discussion, the court focuses on the effect of the clauses and concludes that such clauses, which have similar purposes and effects, are subject to the same disfavor as exculpatory clauses.[28] Under this functional analysis, the hostage clause and the arbitration agreement in Nifty's data processing contract immunize

---

[26] RESTATEMENT (SECOND) OF CONTRACTS § 195(1) (1981).

[27] Southworth & McGill, P.A. v. So. Bell Tel. and Tel. Co., 580 So. 2d 628, 634 (Fla. Dist. Ct. App. 1991) (footnote and citation omitted).

[28] O'Connell v. Walt Disney World Co., 413 So. 2d 444 (Fla. Dist. Ct. App. 1982).

Nifty from the consequences of its tortious conduct and, thus, should be disfavored and subject to careful scrutiny.

To be enforceable against Happy Valley, the intention of the clause must be "clear and unequivocal" and the contractual language must convey in an understandable way the consequences of the clause.[29] Although Happy Valley is in some ways a sophisticated business entity, it is unclear whether the implications of the data hostage clause and arbitration clause taken together were conveyed in a manner that made these consequences clear.[30]

III. TWO STRATEGIES TO MITIGATE THE IMPACT OF DATA HOSTAGE CLAUSES

It is unlikely that service providers will voluntarily stop requiring their outsourcing customers to agree to data hostage clauses. Moreover, outsourcing customers are unlikely to litigate in data hostage situations. It is therefore unlikely that case law will develop in this area to clarify the extent to which data hostage clauses are enforceable. There are two possible solutions to the data hostage dilemma; the first requires government intervention while the second requires addition of a contract term creating a private expedited dispute resolution mechanism to remove the data from the service provider while arbitration or litigation proceeds.

A. Government Intervention

Financial institution regulators might at least prohibit the use of data hostage terms in outsourcing contracts entered into by regulated financial institutions. Federal regulators, particularly those for banking

---

[29] *Id.*

[30] While beyond the scope of this article, it may in fact be possible, at least under Florida's formulation of the law, to construct a data hostage clause and dispute resolution mechanism that overcomes the legal disfavor of such clauses and satisfies requirements for enforceability. *See* Glenn D. West & W. Benton Lewis, Jr., *Contracting to Avoid Extra-Contractual Liability–Can Your Contractual Deal Ever Really Be the "Entire" Deal?*, 64 BUS. LAW. 999 (2009) (examining the effectiveness of exculpatory contract provisions, in the context of fraud and negligent misrepresentation claims, in limiting tort liability).

institutions, may regulate and examine those companies that provide services to Federally-chartered or Federal Deposit Insurance Corporation-insured entities.[31] However, direct regulation in this form (as opposed to examinations that occur on a regular basis) rarely occurs.

Taking a more indirect approach to the problem, financial regulators might promote "best practices" for IT outsourcing. For example, the Federal Deposit Insurance Corporation began requiring insured banks and thrifts to maintain certain deposit data in specific formats, regardless of whether they process the data in-house or outsource the services.[32] Further, the Federal Financial Institutions Examination Council, which is a cooperative of all Federal banking regulators, long ago issued examinations guidance that advises directly on certain substantive terms in IT outsourcing contracts.[33] Federal and state regulators could continue to strengthen their guidance to regulated institutions regarding the dangers of data hostage clauses, or even prohibit their use altogether. This approach could increase data portability for businesses that employ cloud computing services.

B. Private Choice

Parties to IT outsourcing contracts could reduce the leverage service providers enjoy by providing for more expeditious resolution of disputes. This could be done by drafting a rapid resolution mechanism. This mechanism would permit the parties to submit limited evidence to a single, neutral decision maker who is required to decide quickly whether a terminating customer is likely to prevail in arbitration or litigation. The standard could be much like that applied in Federal courts for the issuance of a preliminary injunction, i.e., whether the party seeking the preliminary injunction is "likely to succeed on the merits."[34]

---

[31] *See* 12 U.S.C. §§ 1464(d)(7)(D), 1867(c) (2006).

[32] *See* 12 C.F.R. § 360.9 (2009) (stating the FDIC rule requiring that major banks keep deposit data in specific format to assist in deposit insurance determinations).

[33] *See* OUTSOURCING TECHNOLOGY SERVICES, *supra* note 10, at 12–19.

[34] Winter v. Natural Res. Def. Council, Inc., 129 S. Ct. 365, 374 (2008).

If the neutral decision maker finds that the customer seeking return of its data without payment of the termination fee meets the standard, then the service provider would be compelled to first deliver the data and then submit the dispute to arbitration or litigation, as agreed in the parties' contract. Such a rapid resolution mechanism could be cast as a mandatory, binding arbitration provision that is enforceable pursuant to the Federal Arbitration Act.[35]

CONCLUSION

The data portability discussion among IT cloud computing service providers is a familiar one. Financial institutions have been outsourcing data processing to service providers for years. These service provider arrangements are precursors to the services provided by today's cloud computing companies.

Typical contract provisions that have hindered or even prevented defections from one service provider to another have been problematic for the financial services industry. If they are used in cloud computing, then they may become problematic in other industries as well. Outsourcing businesses may not recognize the coercive power their service providers stand to gain when data hostage clauses are combined with dispute resolution clauses that permit substantial delays in resolving disputes.

In regulated industries, like financial services, regulators can address the problem and adopt remedial measures to discourage or eliminate the unfairness that data hostage clauses impose. In other industries, outsourcing businesses could reduce the risk of paying substantial termination fees, even to service providers that have breached their agreements, by devising expedited dispute resolution terms.

---

[35] *See* AM. BAR ASS'N, MODEL ASSET PURCHASE AGREEMENT WITH COMMENTARY § 2.9 and cmt. (2001) (offering a similar provision to resolve purchase price adjustment disputes in asset purchase transactions and discussing its enforceability as an agreement to arbitrate).

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 6, ISSUE 1 SUMMER 2010

ARBITRATION NATION: WIRELESS SERVICES PROVIDERS AND CLASS ACTION WAIVERS

Alexander J. Casey[*]

CITE AS: 6 WASH J.L. TECH. & ARTS 15 (2010)
https://digital.lib.washington.edu/dspace-law/handle/1773.1/448

ABSTRACT

State consumer protection laws protect the public against unfair and deceptive trade practices. Plaintiffs seeking to invoke such consumer protection laws often bring class action suits to vindicate their rights. However, some jurisdictions have recently shown a willingness to enforce contract arbitration clauses that contain class action waivers. Such waivers prevent consumers from invoking class action status, and may also prevent them from enforcing relevant state consumer protection laws. Other courts, by contrast, have held that service contracts containing class action waivers violate relevant state consumer protection laws and are against public policy. Yet another group of courts facing the issue of class action waiver enforcement has held that relevant federal statutes preempt consumer claims brought under state law. This Article discusses this jurisdictional split on the issue of class action waivers and arbitration as they appear in telecommunication and wireless contracts. This Article also considers the implications of this jurisdictional divide for both businesses and wireless consumers.

---

[*] Alexander J. Casey, University of Washington School of Law, Class of 2010. Thank you to Professor Jane K. Winn of the University of Washington School of Law, and student editors Chelsea Spector and Jennifer Heidt White for their valuable feedback. Thank you also to Professor Jeff Sovern of St. John's University School of Law.

TABLE OF CONTENTS

INTRODUCTION

Class action suits and consumer protection laws, like certain public agencies such as the Federal Trade Commission, have long defended the public from questionable business practices.[1] The Supreme Court has remarked that "the class action mechanism is [designed] to overcome the problem that small recoveries do not provide the incentive for any individual to bring a solo action . . . [and] solves this problem by aggregating the relatively paltry potential recoveries into something worth someone's (usually an attorney's) labor."[2] While there

---

[1] "Where the parties interested in the suit are numerous, their rights and liabilities are so subject to change and fluctuation by death or otherwise, that it would not be possible, without very great inconvenience, to make all of them parties, and would oftentimes prevent the prosecution of the suit to a hearing. For convenience, therefore, and to prevent a failure of justice, a court of equity permits a portion of the parties in interest to represent the entire body, and the decree binds all of them the same as if all were before the court." Thibodeau v. Comcast Corp., 912 A.2d 874, 884 (Pa. Super. Ct. 2006) (citing Smith v. Swormstedt, 57 U.S. (16 How.) 288, 303 (1854)).

[2] Amchem Products, Inc. v. Windsor, 521 U.S. 591, 617 (1997). Judge Posner writes, "[t]he *realistic* alternative to class action is not 17 million individual suits, but

remains an ongoing dialogue about the exact role of class actions within the United States,[3] many contract drafters have sought to limit class actions as a means to resolve contract disputes. These limitations may be accomplished in several ways, including the use of arbitration clauses that contain a class action waiver provision.

Although class action waivers are widely used, such contract language has been the subject of heightened political scrutiny in recent months.[4] Courts are split as to the enforceability of arbitration clauses, especially when a class action waiver is located within that specific clause. There are two bases for the jurisdictional split on the issue of arbitration class action enforcement: federal preemption and substantive state law. First, some courts have held that federal law preempts state law on the issue of arbitration; as federal law favors the enforcement of such arbitration clauses, these courts apply the terms. Other courts have concluded, however, that where there is no issue of federal preemption, the terms of the arbitration clause and its class action waiver may violate state consumer protection laws and public policy. Thus, one split is on the issue of federal preemption and the second split arises over whether a substantive violation of state law has in fact taken place.

In addressing the jurisdictional divisions in telecommunication contracts, this Article briefly discusses the origin of class action consumer protection suits. This Article then addresses the arguments put forth on the issue of federal preemption, as well as the resulting division on the issue of the arbitration clause enforcement. This Article evaluates the leading cases favoring the nullification of class

---

zero individual suits, as only a lunatic or a fanatic sues for $30 dollars." Carnegia v. Household Int'l, Inc., 376 F.3d 656, 661 (7th Cir. 2004).

[3] *See generally* Martin H. Redish, *Class Actions and the Democratic Difficulty: Rethinking the Intersection of Private Litigation and Public Goals*, 2003 U. CHI. LEGAL F. 71 (2003).

[4] *See generally* Arbitration Fairness Act of 2009, H.R. 1020, 111th Cong. (2009), *available at* http://www.thomas.gov/cgi-bin/query/z?c111:H.R.1020: (proposing substantial changes to the Federal Arbitration Act); *cf.* Ashby Jones, *An Arbitration Revolution? AAA Joins NAF, Stops Taking New Cases*, WALL ST. J., Jul. 22, 2009, http://blogs.wsj.com/law/2009/07/22/an-arbitration-revolution-aaa-joins-naf-stops-taking-new-cases/.

action waivers and the conflicting cases that actually reach the substantive legal questions under state law. Finally, this Article discusses the implications of the multifaceted jurisdictional division and its impact on other similarly positioned market actors and telecommunication consumers.

I. ANATOMY OF A SUIT: UNFAIR AND DECEPTIVE TRADE PRACTICES ACTS, PRIVATE ACTORS, AND CONSUMER PROTECTION

Consumer protection laws protect the public from unfair and deceptive business practices in various contexts, including telecommunication agreements between consumers and service providers.[5] Claims against telecommunication providers often arise under state consumer protection acts (CPAs), which are also commonly referred to as unfair and deceptive trade practices acts.[6] Plaintiffs will often assert their CPA rights in addition to their common law contractual rights because punitive damages, statutory damages, and attorney's fees may not be available at common law. Furthermore, a CPA cause of action contains fewer requisite elements than a pure breach-of-contract cause of action.[7]

Plaintiffs pursuing alleged breaches of contract or CPA violations often bring class action lawsuits. Private plaintiffs must, therefore, confront class action waiver language found in their wireless service provider contracts, which may include a specific class action waiver in their contract arbitration clauses. The arbitration clause may contain terms similar to the following:

> Any dispute arising out of this Agreement or relating

---

[5] For example, the Washington state statute broadly provides the following: "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." WASH. REV. CODE § 19.86.020 (2009).

[6] Consumer Protection Acts are also known as "Little FTC [or Federal Trade Commission] Acts." Jeff Sovern, *Private Actions Under the Deceptive Trade Practices Acts: Reconsidering the FTC Act as Model Rule*, 52 OHIO ST. L.J. 437, 438-39 (1991).

[7] *Id.* at 439-40 (explaining that the common law claims of fraud or deceit are often cumbersome in court because the claims involve as many as eight elements).

> to the Services and Equipment must be settled by arbitration by the American Arbitration Association. Each party will bear the cost of preparing and prosecuting its case . . . The arbitrator has no power or authority to alter or modify these Terms and Conditions, including the foregoing Limitations of Liability section. *All claims must be arbitrated individually, and there will be no consolidation or class treatment of any claims*. This provision is subject to the United States Arbitration Act.[8]

In challenging such waivers, plaintiffs have broadly asserted unconscionability-style claims under their relevant state CPA. In other words, plaintiffs asserting their statutory rights often employ language that mirrors the vernacular employed to discuss general contract principles. The concept of "unconscionability," as a term of art, bridges the statutory and common law claims and complicates analysis of the pertinent case law.[9]

For example, in *Iberia Credit Bureau, Inc. v. Cingular Wireless LLC*, the court acknowledged that although plaintiff's challenge to the arbitration clause was "couched in terms of unconscionability, the . . . arguments relate more to broader considerations of public policy than to the harshness of a particular bargain."[10] In *Scott v. Cingular Wireless*, the Washington State Supreme Court similarly observed that "the class action waiver clause . . . is an unconscionable violation of [Washington State] policy to protect the public and foster fair and honest competition" as embodied in Washington's Consumer Protection Act.[11] *Nota bene* the formulation of the claims can implicate

---

[8] Whitney v. Alltel Comms., Inc., 173 S.W.3d 300, 304 (Mo. Ct. App. 2005) (emphasis added).

[9] *See* J. Maria Glover, *Beyond Unconscionability: Class Action Waivers and Mandatory Arbitration Agreements*, 59 VAND. L. REV. 1735, 1757-60 (2006).

[10] Iberia Credit Bureau, Inc. v. Cingular Wireless LLC, 379 F.3d 159, 175 n.20 (5th Cir. 2004).

[11] Scott v. Cingular Wireless, 161 P.3d 1000, 1006 (Wash. 2007) (referencing RCW 19.86.920) (internal quotations omitted).

subsequent class certification proceedings and class representation.[12]

In addition to private causes of action, state attorneys general may also enforce their relevant CPAs.[13] Nevertheless, private citizens functioning as "private attorneys general" also protect the public interest—although not without controversy—when pursuing statutory and common law rights.[14] This rise of private protection of the public interest is due, at least in part, to limited state resources.[15] Although a conflict of interest between private actors and the public good can occur, even in circumstances in which a private party seeks to enforce state law,[16] private actors remain critical to consumer protection.

Consumers challenging the enforceability of arbitration clauses often craft claims alleging, in essence, substantive and procedural unconscionability: (1) the contract "is a contract of adhesion that [(2)] restricts" plaintiff's means of seeking meaningful remedy, (3) because of the inclusion of a class action waiver, (4) that forces plaintiff to participate in cost prohibitive individual arbitration.[17] Courts that have found such a presentation of the issues persuasive have also, generally

---

[12] *Cf.* Schnall v. AT&T Wireless Servs., Inc., 225 P.3d 929, 934, 936-39 (Wash. 2010) (holding that the trial court properly declined certification of a nationwide class action post-*Scott v. Cingular Wireless*, 161 P.3d 1000 (Wash. 2007), where choice of law provisions for each individual contract would require application of multiple states' substantive law so as to overwhelm any common issues; in addition, holding that even as the Washington Consumer Protection Act governs private causes of action, the statute does not extend to protect the interests of citizens from other states).

[13] *See, e.g.*, Press Release, Office of the Attorney General of Minnesota, Attorney General Swanson Sues National Arbitration Company for Deceptive Practices (July 14, 2009), http://www.ag.state.mn.us/Consumer/PressRelease/09 0714National Arbitration.asp.

[14] *See generally* Sovern, *supra* note 7.

[15] *See Scott*, 161 P.3d at 1004; *see also* Kinkel v. Cingular Wireless LLC, 857 N.E.2d 250, 276 (Ill. 2006). *But see* Nina Yadava, Comment, *Can You Hear Me Now? The Courts Send a Stronger Signal Regarding Arbitration Class Action Waivers in Consumer Telecommunication Contracts*, 41 COLUM. J.L. & SOC. PROBS. 547, 574-75 (2008).

[16] Sovern, *supra* note 7, at 438.

[17] Whitney v. Alltel Comms., Inc., 173 S.W.3d 300, 311-12 (Mo. Ct. App. 2005) (citing Leonard v. Terminix Int'l Co., 84 So.2d 529 (Ala. 2002)); *see also* Powertel, Inc., v. Bexley, 743 So.2d 570 (Fla. Dist. Ct. App. 1999).

speaking, found no federal preemption of the relevant state CPA.[18] Nevertheless, federal preemption is a primary defense to these types of telecommunication class action waiver cases, and remains a central sub-issue for many jurisdictions; the jurisdictional split on this sub-issue will be discussed here.

II. FEDERAL PREEMPTION: THE FEDERAL ARBITRATION ACT AND FEDERAL COMMUNICATIONS ACT AS POTENTIAL DEFENSES

Defendants responding to class action suits have claimed the Federal Arbitration Act (FAA), particularly section 2, preempts state consumer protection laws.[19] The Supreme Court has interpreted the final phrase of the statute to require enforcement of arbitration agreements when there remains "evidence [of] a transaction involving commerce, unless [the contract is] revocable on other grounds."[20] Contract defenses "such as fraud, duress or unconscionability, may be applied to invalidate arbitration agreements without contravening [the section]."[21] In other words, an arbitration agreement under the FAA is enforceable unless other grounds—including unconscionability—provide a basis for the contract's invalidation.

The Court provides the additional caveat regarding preemption of state law: "a court may not . . . construe that agreement in a manner different from that in which it otherwise construes nonarbitration agreements under state law. Nor may a court rely on the uniqueness of an agreement to arbitrate as a basis for a state-law holding that

---

[18] *See, e.g.*, *Scott*, 161 P.3d at 1009; *see also* Fiser v. Dell Computer Corp., 188 P.3d 1215 (N.M. 2008) (considering arbitration and class action waiver unconscionability and violation of public policy in the context of computer sales contracts).

[19] Section 2 relevantly provides the following: "A written provision . . . [in] a contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction . . . shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." 9 U.S.C. § 2 (2006).

[20] Thibodeau v. Comcast Corp., 912 A.2d 874, 880 (Pa. Super. Ct. 2006) (citing Southland Corp. v. Keating, 465 U.S. 1, 11-12 (1984)).

[21] Doctor's Assocs., Inc. v. Casarotto, 517 U.S. 681, 687 (1996).

enforcement would be unconscionable . . . ."[22] Stated alternatively, a state law that discriminates specifically against a contract to arbitrate violates section 2 and is likely preempted.

In light of this guidance, lower courts have held that unconscionability, as a *general* contracts principle—and not a *specific* state-law principle or defense devised for arbitration contracts alone—may provide a basis to challenge arbitration provisions.[23] As such, the FAA likely does not preempt state consumer protection law on the issue of class action waivers, except where state law establishes a right to pursue class actions that is statutorily impossible to waive, such as those contained in arbitration provisions.[24] Nevertheless, the Federal Communications Act may still preempt relevant state law on this issue.[25]

A. Federal Preemption Under the Federal Communications Act

Notwithstanding the general consensus on the unavailability of a FAA preemption defense, there remains a second and more persuasive argument for federal governance of this issue under the Federal Communications Act (FCA). The FCA, originally passed in 1934, provides one basis for a jurisdictional division on the enforceability of class action waivers contained within arbitration clauses. In its pertinent section, the FCA prohibits unreasonable discrimination and

---

[22] Iberia Credit Bureau, Inc. v. Cingular Wireless LLC, 379 F.3d 159, 167 (5th Cir. 2004) (citing Perry v. Thomas, 482 U.S. 483, 493 n.9 (1987)) (first alteration in the original).

[23] Lowden v. T-Mobile USA, Inc., 512 F.3d 1213, 1221-22 (9th Cir. 2008); Shroyer v. New Cingular Wireless Servs., Inc., 498 F.3d 976, 988 (9th Cir. 2007); *Scott*, 161 P.3d at 1008 ("Congress simply requires us to put arbitration clauses on the same footing as other contracts, not make them the special favorites of the law.")

[24] *See* Ting v. AT&T, 319 F.3d 1126, 1150 n.15 (9th Cir. 2003) (recognizing the FAA preempts the California Legal Remedies Act (CLRA) creating a statutory right to class action). One could construe CLRA as having discriminated against arbitration contracts particularly as such contracts are often the source of class action waivers.

[25] One should be careful to distinguish between federal preemption of arbitration clauses under the FAA and the preemption of state-law bans on class action waivers that appear in arbitration clauses.

undue preferences among users of interstate services:

> It shall be unlawful for any common carrier to make any unjust or unreasonable discrimination in charges, practices, classifications, regulations, facilities, or services for or in connection with like communication service . . . by any means or device, or to make or give any undue or unreasonable preference or advantage to any particular person, class of persons, or locality, or to subject any particular person, class of persons . . . to any undue or unreasonable prejudice or disadvantage.[26]

The Seventh Circuit, for example, held the FCA impliedly preempts state contract law because, under the text's plain language, a converse holding would encourage price discrimination against consumers in states where arbitration provisions are not enforceable; such discrimination is prohibited under sections 201-202 of the FCA.[27] Nevertheless, other courts have held that no such federal preemption exists.[28]

For example, the Ninth Circuit has held that the Telecommunications Act of 1996, an amendment to the FCA, eliminated any preemption issues that existed under the FCA by removing tariff-filing requirements.[29] This detariffing released any federal preemption

---

[26] 47 U.S.C. § 202(a) (2006).

[27] *See, e.g.*, Boomer v. AT & T Corp., 309 F.3d 404, 423 (7th Cir. 2002); *see also* Dreamscape Design, Inc. v. Affinity Network, Inc., 414 F.3d 665, 674 (7th Cir. 2005) (holding the same).

[28] *See, e.g.*, *Ting*, 319 F.3d at 1139-43 (holding there is no implied federal preemption under the FCA); McKee v. AT & T Corp. 191 P.3d 845, 855 (Wash. 2008) (holding the same).

[29] *Ting*, 319 F.3d at 1139. Historically, "Section 203 of the Communications Act of 1934 (the 1934 Act) require[d] all common carriers to file tariffs showing all charges for the interstate and foreign wire or radio communications services they provide[d], as well as the classifications, practices, and regulations affecting such charges." Charles H. Helein, Jonathan S. Marashlian & Loubna W. Haddad, *Detariffing and the Death of the Filed Tariff Doctrine: Deregulating in the "Self" Interest*, 54 FED. COMM. L.J. 281, 287 (2008). The FCC began detariffing in the 1980s by removing the required filing processes, and continued the process until July 2001. *Id.*

concerns because federal regulation of the telecommunications industry ceased, and instead shifted to state and common law.[30] This shift of legal authority created another court split regarding whether class action waiver terms *actually* violate the controlling state CPA.[31] It is this second split that will be the focus of the next section.

III. ARBITRATION CLAUSES AND "UNCONSCIONABILITY": THE CENTRAL ISSUE

Numerous courts have held that class action waivers, particularly as they appear in both wireless service provider contracts and other telecommunication related contracts, are unconscionable and against public policy.[32] In general, courts analyzing the issue focus on two broad factors—procedural unconscionability and substantive unconscionability—which together can be considered a "totality of the circumstances" approach that requires proving both elements before a

---

at 288.

[30] *Ting*, 319 F.3d at 1139; *McKee*, 191 P.3d at 855.

[31] *See generally* Alan S. Kaplinsky, Mark Levin & Martin C. Bryce Jr., *Arbitration Developments: The Battle Against Arbitration Intensifies*, 65 BUS. LAW. 657 (2010); *see also* Alan S. Kaplinsky, *A Scorecard on Where Federal and State Appellate Courts and Statutes Stand on Enforcing Class Action Waivers in Pre-dispute Consumer Arbitration Agreements*, 1591 PRAC. L. INST./CORP. 9 (2007).

[32] *See, e.g.*, Lowden v. T-Mobile USA, Inc., 512 F.3d 1213 (9th Cir. 2008) (applying California law); Dale v. Comcast Corp., 498 F.3d 1216 (11th Cir. 2007) (applying Georgia law); Kristian v. Comcast Corp., 446 F.3d 25 (1st Cir. 2006) (holding against class action waiver enforcement for telecommunication services contract); Ting v. AT&T, 319 F.3d 1126 (9th Cir. 2003) (applying California law); Bradberry v. T-Mobile USA, Inc., No. C 06-6567 CW, 2007 WL 1241936 (N.D. Cal. Apr. 27, 2007) (applying California law); Scott v. Cingular Wireless, 161 P.3d 1000 (Wash. 2007); Kinkel v. Cingular Wireless LLC, 857 N.E.2d 250 (Ill. 2006); Whitney v. Alltel Comms., Inc., 173 S.W.3d 300 (Mo. Ct. App. 2005); Vasquez-Lopez v. Beneficial Or., Inc., 152 P.3d 940 (Or. Ct. App. 2007) (holding against class action waiver enforcement in a lending contract); Discover Bank v. Superior Court, 113 P.3d 1100 (Cal. 2005) (holding against class action waiver enforcement in credit card service contract under California law), *enforced*, 36 Cal. Rptr. 3d 456 (Cal. Ct. App. 2005) (holding (1) that Delaware law was controlling, and (2) the class action waiver was enforceable under Delaware law).

provision will be struck down.[33] Courts may inquire into procedural unconscionability by determining whether the contract is one of adhesion.

As a general matter, an adhesion contract is negotiated by parties with vastly disparate bargaining power, and is often a "pre-printed form contract[]."[34] As the *Whitney v. Alltel Communications* Court notes, however, in an age of "mass production-mass consumer society," such form contracts are commonplace and are not procedurally unconscionable or against public policy per se.[35] Rather, procedural unconscionability hinges on a factual inquiry into the clarity of the contract and a determination of whether it could be easily understood by a consumer.[36] Adhesion contracts, due to their tendency to favor drafters, heighten the court's awareness of potential substantive unconscionability contained in the contract terms, even where such contracts are not typographically unconscionable.[37]

---

[33] *See, e.g.*, Whitney v. Alltel Comms., Inc., 173 S.W.3d 300, 309 (Mo. Ct. App. 2005); *see also* Davidson v. Cingular Wireless LLC, No. 2:06CV00133-WRW, 2007 WL 896349, at *5 (E.D. Ark. Mar. 23, 2007) (employing a similar analysis in a case with an individual plaintiff rather than a class of similar plaintiffs). Some decisions consider only one element of unconscionability—either procedural or substantive, but not both. *Compare* Scott v. Cingular Wireless, 161 P.3d 1000, 1006 n.4 (Wash. 2007) (finding only substantive unconscionability and declining to inquire into procedural unconscionability) *with* Dale v. Comcast Corp., 498 F.3d 1216, 1219 (11th Cir. 2007) (discussing both aspects of unconscionability).

[34] *Whitney*, 173 S.W.3d at 310 (citing Swain v. Auto Servs., Inc., 128 S.W.3d 103, 107 (Mo. Ct. App. 2003)).

[35] *Id.*

[36] *Scott*, 161 P.3d at 1006 n.4 (recounting the factual determination of the lower court but not addressing the issue of adhesion on appeal); *see also* Davidson v. Cingular Wireless LLC, No. 2:06CV00133-WRW, 2007 WL 896349, at *6 (E.D. Ark. Mar. 23, 2007) (considering take-it-or-leave-it clauses, font size, and location of the clauses as potential factors for consideration of procedural unconscionability in case brought by individual plaintiff).

[37] This may be the case despite some guidance that "[a] court may not . . . in assessing the rights of litigants to enforce an arbitration agreement, construe that agreement in a manner different from that in which it otherwise construes nonarbitration agreements under state law." Iberia Credit Bureau, Inc. v. Cingular Wireless LLC, 379 F.3d 159, 167 (5th Cir. 2004) (citing Perry v. Thomas, 482 U.S. 483, 493 n.9 (1987)).

In contrast, courts consider substantive unconscionability by inquiring whether the costs of arbitration are sufficiently low and the availability of compensation adequately high to offer a meaningful remedy.[38] For example, in *Scott v. Cingular Wireless*, the Washington State Supreme Court reasoned that the class action waiver "dramatically" curbed "the public's ability" to protect itself and was, therefore, substantively unconscionable.[39] Because of the cost-prohibitive nature of individual arbitration, the court held that consumers would be unable to vindicate their statutory rights available under Washington's Consumer Protection Act.[40]

In addition, the *Scott* Court took further steps to address the cost-benefit concerns of the plaintiffs. The court declined to view Cingular's contractual offer to shift the administrative costs of arbitration to the defendant as being sufficient inducement to arbitrate, due to the remaining heavy cost placed on the consumer in the form of attorney fees.[41] Furthermore, the *Scott* Court also shed light onto the "meaningful remedy" analysis.

The court reasoned that enforcing the terms of the contract would result in decreased likelihood of representation because "a plaintiff could recover 99 percent of a claim and still not be awarded any

---

[38] *Whitney*, 173 S.W.3d at 311; *Scott*, 161 P.3d at 1006-07.

[39] *Scott*, 161 P.3d at 1003-06 (providing the relevant contract language as follows: "You agree that, by entering into this Agreement, you and Cingular are waiving the right to a trial by jury.... You and Cingular agree that YOU AND CINGULAR MAY BRING CLAIMS AGAINST THE OTHER ONLY IN YOUR OR ITS INDIVIDUAL CAPACITY, and not as a plaintiff or class member in any purported class or representative proceeding. Further, you agree that the arbitrator may not consolidate proceedings [on] more than one person's claims, and may not otherwise preside over any form of a representative or class proceeding, and that . . . if this specific proviso is found to be unenforceable, then the entirety of this arbitration clause shall be null and void.") (original emphasis).

[40] *Id.* at 1005-06 (applying RCW 19.86.020 and its sister statutes).

[41] *Id.* at 1007-08 (observing that as the evidence was presented in the lower court, no arbitration claims had been filed by a Washington State customer against Cingular Wireless for the six years preceding this litigation). Other courts relied on by the majority lacked a factual scenario in which there was a contractual obligation imposed upon the defendant to pay the arbitration administrative fees. *See, e.g.*, *Whitney*, 173 S.W.3d at 313-14.

attorney fees."[42] More broadly, the difficulty of acquiring counsel to accept such cases with little to no possibility of financial compensation effectively insulates the contractor from damages available in a CPA claim and breach of contract claim.[43] While the court conceded that attorneys fees are formally available in arbitration, a class action waiver allocates the entire risk of litigation costs to the individual consumer, while offering relatively marginal gain.[44] As such, the class action waiver economically deters suits seeking redress for "a broad range of undefined wrongful conduct."[45]

Higher courts, holding class action waivers to be unconscionable, have repeatedly stated that the substantive unconscionability of each contract is fact-specific and the holding should not be understood as a blanket voidance of all other similar contracts.[46] For contractors, this may indicate that courts that have held against the enforceability of class action waivers would be willing to reconsider contracts that offer greater opportunities to pursue a meaningful remedy. As yet, however, the exact terrain and language of such a contract remains unknown—drafters should be very wary.

IV. DECISIONS FAVORING THE ENFORCEMENT OF ARBITRATION CONTRACTS DUE TO AN ABSENCE OF "UNCONSCIONABILITY"

While there exists substantial precedent supporting the invalidation of class action waivers in telecommunication service agreements, there is also support for the enforcement of such contracts.[47] For

---

[42] *Scott*, 161 P.3d at 1007.

[43] *Id.*

[44] *Id.*

[45] *Id.* at 1007-08.

[46] *Compare* Lowden v. T-Mobile USA, Inc., 512 F.3d 1213, 1215 (9th Cir. 2008) (alleging that defendant had imposed improper charges relating to free services, additional fees beyond the advertised price, and improperly tallied plaintiffs' roaming charges), *with* Riensche v. Cingular Wireless LLC, No. C06-1325Z, 2007 WL 3407137, at *2-3 (W.D. Wash. Nov. 9, 2007) (alleging that defendants improperly transferred a "State B and O Surcharge" that was imposed by the State of Washington, directly to the consumers).

[47] "Generally applicable contract defenses, such as fraud, duress, or

example, in *Iberia Credit Bureau, Inc. v. Cingular Wireless*, the plaintiffs asserted claims against several telecommunications providers, including Cingular Wireless; the claims included both alleged violations of the Louisiana Unfair Practices Act as well as breach of contract. The court considered both the procedural and substantive components of unconscionability, as required under Louisiana law.[48]

Under the procedural element of unconscionability, the *Iberia Credit* Court considered and rejected the size of the font as a valid basis for holding that the contract was one of adhesion.[49] Under the substantive unconscionability prong, the court noted that "the Louisiana Unfair Trade Practices Act (LUTPA) . . . does not permit individuals to bring class actions. Although this prohibition does not apply to the plaintiffs' breach-of-contract cause of action, it does significantly diminish the plaintiffs' argument that prohibiting class proceedings in consumer litigation is unconscionable under Louisiana law."[50] The court then elaborated on the possible availability of alternative remedies for consumers to pursue in support of their substantive analysis.[51] Regardless, under the Fifth Circuit's treatment of Louisiana law, class action waivers do not render arbitration provisions unconscionable.[52] When considered in light of other cases

---

unconscionability, may be applied to invalidate arbitration agreements without contravening," but such agreements are otherwise enforceable. Iberia Credit Bureau, Inc. v. Cingular Wireless LLC, 379 F.3d 159, 166 (5th Cir. 2004) (citing Doctor's Assocs. v. Casarotta, 517 U.S. 681, 687 (1996)).

[48] *Id.* at 167.

[49] *Id.* at 172.

[50] *Id.* at 174-75 (internal citations omitted); *see also* LA. REV. STAT. ANN. § 51:1409(A) (2008) (granting an individual the right to sue in a non-representative capacity).

[51] *Iberia Credit Bureau*, 379 F.3d at 177 n.19 (discussing the availability of small claims actions as a viable remedy for consumers as well as the right of the Attorney General to sue on behalf of aggrieved consumers). Nevertheless, some states prohibit counsel in small claims court. *See, e.g.*, Arkansas Judiciary, Small Claims Court in Arkansas (2008), courts.arkansas.gov/documents/small_claims_info.pdf; *see also* Davidson v. Cingular Wireless LLC, No. 2:06CV00133-WRW, 2007 WL 896349, at *6 (E.D. Ark. Mar. 23, 2007) (considering similar options with an individual plaintiff).

[52] *Iberia Credit Bureau*, 379 F.3d at 175.

on this issue, the *Iberia Credit* Court's holding and the resulting jurisdictional divide have widespread implications.

V. WHERE TO GO FROM HERE: IMPLICATIONS AND OBSERVATIONS

As the *Vasquez* Court observed nearly 40 years ago: "[a] class action by consumers produces several salutary *by-products*, including a therapeutic effect upon those sellers who indulge in fraudulent practices, aid to legitimate business enterprises by curtailing illegitimate competition, and avoidance to the judicial process of the burden of multiple litigation involving identical claims. The benefit to the parties and the courts would, in many circumstances, be substantial."[53] A jurisdictional split on the issue of class action waivers has implications for wireless service providers, other similarly situated telecommunication companies, and consumers.

First, smaller providers that have yet to deploy class action waivers in their service provider contracts are likely to be at a competitive disadvantage within the telecommunications market. In addition, the inclusion of a class action waiver in a service provider contract may still, as the case law suggests, fail to insulate the corporation from liability for certain trade practices. Given these considerations, a cost-benefit analysis for each provider would be necessary to assess the proper course of action regarding the inclusion of such a waiver. Naturally, such a waiver does not necessarily prevent arbitration.

Furthermore, favoring arbitration and enforcement of class action waivers will likely diminish overall public awareness of dubious business practices against both individual consumers and non-telecommunication businesses. As the *Scott* Court noted, "many consumers may not even realize that they have a claim" without a class action suit; moreover such consumers are not only single individuals, but often small businesses and the like.[54] Telecommunications

---

[53] Vasquez v. Super. Ct. of San Joaquin County, 484 P.2d 964, 968-69 (Cal. 1971) (emphasis added).

[54] Scott v. Cingular Wireless, 161 P.3d 1000, 1006-07 (Wash. 2007) (citing Abels v. JBC Legal Group, PC, 227 F.R.D. 541, 547 (N.D. Cal. 2005)); *see also* Iberia Credit Bureau, Inc. v. Cingular Wireless LLC, 379 F.3d 159, 163 (5th Cir. 2004)

corporations may, therefore, calculate that the likelihood of class action waiver being invalidated is sufficiently low to continue using them, notwithstanding the risk of litigation over the validity of the clauses. Or still more troublesome, such corporations may calculate that the damages resulting from a losing suit are still sufficiently low so as to justify the use of class action waivers against customers in other arbitration-enforcing jurisdictions.[55] Consumers should be on the look out.

In addition, courts that inquire into the business practices of the wireless service providers will likely affect both public and private actors in the future. The *Iberia Credit* Court noted that telecommunication provider contracts might also include a confidentiality clause within their arbitration clauses.[56] Indeed, confidentiality clauses can limit the parties from disclosing the results of arbitration. Furthermore, arbitration "depriv[es] plaintiffs of the ability to establish precedent."[57] The result will likely be that consumers in the future, especially in particular jurisdictions where arbitrations are still widely practiced, will be less able to know and invoke their available rights under state consumer protection laws.

Finally, the implications of widespread denial of class actions may require state attorneys general, or state legislatures, to take a more active role in this area of the law to prevent continued use of questionable practices by telecommunications companies. On the

---

(enforcing a contract in which neither party "may disclose the existence, content or results of any arbitration . . . .").

[55] The ethical questions raised by advising a client to retain an unconscionable provision in a jurisdiction that, for example, claims to follow a case-by-case approach to contract arbitration issues, remain beyond the scope of this Article.

[56] Iberia Credit Bureau, Inc. v. Cingular Wireless LLC, 379 F.3d 159, 175 (5th Cir. 2004).

[57] *Id. But see, e.g.*, Chambers v. Capital Cities/ABC, 159 F.R.D. 441, 445 (S.D.N.Y. 1995) (finding against the enforceability of a confidentiality agreements with regards to a discrimination claim, but not trade secret claims; also observing that "[w]here conduct of a party tends to preclude availability of information relevant to a litigation and where no genuine basis for keeping that information confidential exists, a court or factfinder may infer that the information, if disclosed, would be contrary to the position of the party engaging in such conduct." (citing Baxter v. Palmigiano, 425 U.S. 308, 316-20 (1976))).

other hand, even where states have invalidated class action waivers, additional considerations still arise, including: nationwide class actions and the extraterritorial extension of state statutes to protect foreign citizens from the acts of telecommunication companies operating or incorporated in the forum jurisdiction.[58] Regardless, state attorneys general should take a more active enforcement role to combat the unfair trade practices altogether.[59]

CONCLUSION

The continued appearance of class action waivers in the arbitration clauses of telecommunication contracts may deter individual consumers from exercising their legal rights. Indeed, only exceedingly provoked consumers would believe it possible to recoup such a paltry sum after reading their arbitration clauses.[60] Nevertheless, rulings such

---

[58] *See, e.g.*, Schnall v. AT&T Wireless Servs., Inc., 225 P.3d 929, 936-39 (Wash. 2010) (Madsen, C.J.) (holding, as was noted, that the trial court properly declined certification of a nationwide class action where choice of law provisions for each individual contract would require application of multiple states' substantive law so as to overwhelm any common issues; in addition, holding that even as the Washington consumer protection act governs private causes of action, the statute does not extend to protect the interests of the citizens from other states) (internal citations and quotations omitted).

[59] In states such as Washington, as the dissent in *Scott* pointed out, state legislatures could, and arguably should, be the legal body to address the consistency problem of class action waivers in arbitration clauses and other derivative issues such as nationwide class action suits and class arbitration. *Scott*, 161 P.3d at 1010-11 (Madsen, J., dissenting) (comparing the California legislature's explicit addressing of the issue of class action waivers compared to the majority's policy rationales). It should be noted, however, that the issue of federal preemption looms large over the state legislature's authority to address the issue. *See* Donald M. Falk & Archis A. Parasharami, *Federal Court Rejects Class Action Waivers in Arbitration Clauses*, 14 WASH. LEGAL FOUND. 8 (2006), *available at* http://www.wlf.org/upload/100606falk.pdf (highlighting the risks of compelled class arbitration as a result of cases in this area of the law).

[60] *See, e.g.*, Carnegie v. Household Int'l, Inc., 376 F.3d 656, 661 (7th Cir. 2004); *see also* Thibodeau v. Comcast Corp., 912 A.2d 874, 885 (Pa. Super. Ct. 2006). This, of course, presumes that the consumer reads the arbitration provision in the first instance or is aware of the extent to which such a provision reduces the likelihood of

as *Scott v. Cingular Wireless* should put individual wireless consumers, including small business owners and other non-traditional consumers, on notice that: (1) clauses within their service provider contracts may be void as per public policy; (2) a public record has been developed on such issues that has not been sealed by an arbitrator; (3) the terms of such contracts may change to circumnavigate such jurisdictions and states via the use of choice of law provisions; and (4) class arbitration may be on the way. Moving forward, consumers and advocates alike will need to be both sensitive to a sharp divide in the treatment of arbitration provisions and class action waivers, and strategic when pursuing potential claims—class action or otherwise—against telecommunication providers.

---

successfully litigating a dispute.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 6, ISSUE 1 SUMMER 2010

MOBILE MARKETING DERAILED: HOW CURBING CELL-PHONE SPAM IN *SATTERFIELD V. SIMON & SCHUSTER* MAY HAVE BANNED TEXT-MESSAGE ADVERTISING

Gareth S. Lacy[*]

CITE AS: 6 WASH J.L. TECH. & ARTS 33 (2010)
https://digital.lib.washington.edu/dspace-law/handle/1773.1/450

ABSTRACT

The risk of receiving cell-phone spam—in the form of unsolicited text messages—grows as advertisers increasingly target cell-phone users. The Telephone Consumer Protection Act of 1991 (TCPA) clearly prohibits unsolicited telephone calls made by an automated telephone dialing system (ATDS) without the recipient's express prior consent. But until the Ninth Circuit's decision in Satterfield v. Simon & Schuster, it was unclear how TCPA applied to text messages. Simon & Schuster argued their text messages were not "calls" under the TCPA and were not sent by an ATDS. The Ninth Circuit disagreed and held a text message is a "call." The court also held an ATDS means any equipment with capacity to store or dial random or sequential telephone numbers, regardless of whether such calls were actually made. This sweeping rule arguably applies to any computer. The court also adopted narrow legal definitions of "brand" and "affiliate" that could hinder any business seeking third-party advertisers to send messages on its behalf. This Article explores how Satterfield exposes mobile advertisers to significantly increased liability.

---

[*] Gareth S. Lacy, University of Washington School of Law, Class of 2011. Thank you Professor Jane K. Winn of the University of Washington School of Law and Thomas Hackett, Article Editor, for offering valuable feedback. Thank you also to Matthew Staples, Associate, Wilson Sonsini Goodrich & Rosati, for sharing his expertise in this area of law.

TABLE OF CONTENTS

INTRODUCTION

In 2004 Laci Satterfield downloaded a free ringtone for her eight-year-old son's cell phone from www.nextones.com.[1] Two years later publishing giant Simon & Schuster launched an advertising campaign using text messages to promote Stephen King's latest horror novel, *Cell*.[2] The company outsourced the advertising to ipsh!, Inc. (ipsh!), a mobile marketing firm with 100,000 cell-phone numbers purchased from various Web sites including Nextones.[3]

At half-past midnight on January 18, 2006, Satterfield's son

---

[1] Satterfield v. Simon & Schuster, Inc., 569 F.3d 946, 949 (9th Cir. 2009); Brief for Defendants-Apellees at 4., Satterfield v. Simon & Schuster, Inc., 569 F.3d 946 (9th Cir. 2009) (No. 07-16356), 2007 WL 4856754.

[2] Jeffrey A. Trachtenberg, *Stephen King Tries to Ring Up Book Sales*, WALL ST. J., Jan. 23, 2006, at B1. (King's book is about a supernatural force transforming the world's cell-phone users into flesh-eating zombies.) *See* Janet Maslin, *Invasion of the Ring Tone Snatchers*, N.Y. TIMES, Jan. 23, 2006, at E1 *available at* http://www.nytimes.com/2006/01/23/books/23masl.html.

[3] Before downloading the ringtone, Satterfield had checked a box next to the following statement: "Yes! I would like to receive promotions from Nextones affiliates and brands. Please note, that by declining you may not be eligible for our FREE content. By checking Submit, you agree that you have read and agreed to the Terms and Conditions." Satterfield v. Simon & Schuster, 569 F.3d at 949.

received Simon & Schuster's text-message advertisement:

> The next call you take may be your last . . . Join the Stephen King VIP Mobile Club at www.cellthebook.com. RplySTOP2OptOut. PwdbyNexton.[4]

The message terrified the young boy. Satterfield wrote "STOP" in response. Then she sued Simon & Schuster and ipsh![5] for sending an unsolicited text-message advertisement in violation of the Telephone Consumer Protection Act of 1991 (TCPA).[6] She later sought to certify a class of 60,000 people who received similar messages.[7]

Simon & Schuster moved for summary judgment by arguing: TCPA did not apply because text messages were not "calls," the messages were not sent by a prohibited ATDS, and Satterfield consented to receive promotions from Nextones affiliates and brands.[8] The district court ruled for Simon & Schuster.[9] But the Ninth Circuit reversed and held: (1) a text message is a "call" under TCPA; (2) an ATDS is any equipment with capacity to store, produce, or call random or sequential numbers; and (3) Simon & Schuster was not an "affiliate" or "brand" of Nextones and therefore Satterfield did not consent to receive the text-message advertising.[10] The decision reinstated Satterfield's effort to certify a $90-million class action lawsuit.[11]

This Article will describe the laws regulating text-message

---

[4] *Satterfield*, 569 F.3d at 949.

[5] Corrected Complaint for Damages and Injunctive Relief at 1, Satterfield v. Simon & Schuster, Inc., No. C 06-2893 CW (N.D. Cal. June 26, 2007), 2006 WL 1787153, *rev'd*, 569 F.3d 946 (9th Cir. 2009).

[6] 47 U.S.C. § 227 (2006) *et seq.*

[7] First Amended Class Action Complaint for Damages and Injunctive Relief, Satterfield v. Simon & Schuster, Inc., No. 406CV02893 (N.D. Cal. Sep. 17, 2009), 2009 WL 3441944; *9th Cir. Hangs Up on Text Message Spam*, 16 No. 7 ANDREWS CLASS ACTION LITIG. REP. 23 (Aug. 19, 2009).

[8] *Satterfield*, 569 F.3d at 950.

[9] *Id.*

[10] *Id.* at 951, 952, 955.

[11] *9th Cir. Hangs Up on Text Message Spam*, 16 No. 7 ANDREWS CLASS ACTION LITIG. REP. 23 (Aug. 19, 2009).

advertising and will explore how *Satterfield v. Simon & Schuster* exposes mobile advertisers to liability under TCPA. In particular, the court's broad definition of a prohibited ATDS—any computer with capacity to generate random numbers—may further restrict text-message marketing. The court's definitions of "affiliate" and "brand" may also discourage the use of plain language in terms and conditions displayed to consumers visiting Web sites.

I. TEXT-MESSAGE ADVERTISING AND MOBILE SPAM PREVALENCE

Text messaging, or short message service (SMS), allows cell-phone users to send and receive 160-character text-only messages.[12] Carriers charge per text message or offer monthly flat rates.[13] SMS supports sending messages phone-to-phone or Internet-to-phone.[14] Phone-to-phone messages are directed to cell-phone numbers. Internet-to-phone messaging allows users to send their message to an e-mail address assigned by the wireless carrier; the carrier then converts this e-mail into a text message.[15]

Text messaging is big business. In 2008 American cell-phone users sent an average of seven billion text messages per month, up 20 percent from 2007.[16] The mobile advertising market, including text-

---

[12] The European Telecommunication Standards Institute (ETSI) first developed an SMS technical standard in the early 1990s. Today the Third Generation Partnership Project (3GPP) develops and maintains an SMS standard inter-nationally. *See* 3rd Generation Partnership Project, Technical Realization of Short Message Service (SMS), Technical Report 3GPP TS 23.040, http://www.3g pp.org/specification-numbering (last visited Apr. 24, 2010).

[13] Steven Masur & John Maher, *Mobile Phone Text Message Spam: Building A Vibrant Market for Mobile Advertising While Keeping Customers Happy*, 7 VA. SPORTS & ENT. L. J. 41, 44-45 (2007).

[14] Joffe v. Acacia Mortgage Co., 121 P.3d 831, 837-38 (2005).

[15] Every cell-phone number has an e-mail address that is typically the user's cell-phone number and the wireless carrier's domain address. For example, the AT&T cell-phone number (783) 836-5464 would have an e-mail address: 7838365464@att. wireless.net. E-mails sent to that address would be converted to text message and then delivered to the user's cell phone. *See Joffe*, 121 P.3d at 837-38.

[16] Liz Farmer, *Conn.-based Vesta Mobile hoping u r ready 4 txt msg mrktng*, DAILY

message marketing, is projected to be worth $12 billion by 2011.[17] Text messaging is now more popular than cell phone calls.[18]

A broad range of technology providers are involved in creating, processing, and distributing text-message advertising.[19] In *Satterfield*, for example, five companies accessed Satterfield's phone number before she received the text-message advertisement.[20] In an effort to self-regulate, more than 600 carriers, advertisers, manufacturers, and software providers formed the Mobile Marketing Association (MMA) in 2000 to issue voluntary best practices guidelines for the mobile advertising industry.[21]

Despite these efforts, private lawsuits alleging spam text messaging (also known as wireless spam, cellular spam, mobile spam or m-spam)

REC. (Baltimore), Mar. 27, 2008, *available at* http://findarticles.com/p/articles/mi_qn4183/is_20080327/ai_n24975493.

[17] Susan Moore, *Gartner Says Telecom Carriers Are Well Placed to Win Advertising Revenue if They Overcome Key Challenges*, GARTNER NEWSROOM, Aug. 26, 2008, http://www.gartner.com/it/page.jsp?id=747112.

[18] Priya Ganapati, *Texting Finally More Popular Than Calling Among U.S. Mobile Users*, WIRED, Sep. 22, 2008, http://www.wired.com/gadgetlab/2008/09/us-finally-catc/.

[19] Linda A. Goldstein, *Mobile Advertising and Web 2.0*, 962 PRAC. L. INST./PAT. 315, 324 (2009); *see also* MOBILE MARKETING ASSOCIATION, UNDERSTANDING MOBILE MARKETING: TECHNOLOGY & REACH (May 2007), *available at* http://www.mmaglobal.com/uploads/MMAMobileMarketing102.pdf.

[20] Satterfield v. Simon & Schuster, Inc., 569 F.3d 946, 950 (9th Cir. 2009). First, Nextones sold customer phone numbers to MIA. MIA then sold those numbers to ipsh!, the mobile advertising company Simon & Schuster hired. Employees at ipsh! wrote the text messages for Simon & Schuster and converted them to a file format deliverable to wireless carriers. Those files—embedded with telephone numbers—were sent to mBlox, a mobile transaction networking service company or "aggregator." (Aggregators combine, on one network, all direct communications to wireless carriers.) mBlox transmitted the messages to carriers that routed them to customers. *See generally* Eric Goldman, *Ninth Circuit Revives TCPA Claim-Satterfield v. Simon & Schuster*, TECHNOLOGY & MARKETING LAW BLOG, July 3, 2009, http://blog.ericgoldman.org/archives/2009/07/ninth_circuit _r.htm (last visited Apr. 10, 2010).

[21] MOBILE MARKETING ASSOCIATION, U.S. CONSUMER BEST PRACTICES GUIDELINES VERSION 5.0 (June 1, 2010), http://www.mmaglobal.com/bestpractices.pdf [hereinafter GUIDELINES].

continue to target mobile advertisers.[22] American cell-phone users received 1.5 billion spam messages in 2008—a 37 percent increase from the 1.1 billion messages received in 2007.[23]

II. HOW *SATTERFIELD* RESTRICTS MOBILE ADVERTISING

Two federal laws regulate text-message advertising: (1) TCPA[24] and its FCC regulations[25]; and (2) the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)[26] and its FCC regulations.[27] TCPA permits private lawsuits[28] and does not preempt state anti-spam laws.[29] In contrast, CAN-SPAM generally prohibits private lawsuits[30] and preempts most state law.[31] *Satterfield* ultimately

---

[22] Jack Gordon, *FDCPA and Other Consumer Rights Lawsuit Statistics*, WEBRECON LLC, Jan. 7, 2010, http://webrecon.com/news/?p=131; Bridget M. O'Neill, *Wireless Spam This Way Comes: An Analysis of the Spread of Wireless Spam and Proposed Measures to Stop It*, 22 J. MARSHALL J. COMPUTER & INFO. L. 229 (2003).

[23] Richi Jennings, *SMS Text Message Spam is a Minor Problem*, FERRIS RESEARCH BLOG, July 14, 2008, http://www.ferris.com/2008/07/14/sms-text-message-spam-is-a-minor-problem/. Jennings argues U.S. cell-phone spam is still rare relative to other countries; approximately one-third of one percent of total U.S. messages were spam in 2007. But cell-phone spam has become a significant problem internationally. For example, 200 million Chinese cell-phone users received spam text messages in 2008. *Beijing Investigates Spam Attack*, BBC WORLD NEWS, http://news.bbc.co.uk/2/hi/business/7311242.stm (March 24, 2008); *see also* Terrence O'Brien, *Text-Message Spam Continues to Grow Around the World*, SWITCHED, May 4, 2009, http://www.switched.com/2009/05/04/text-message-spam-continues-to-grow-around-the-world/.

[24] 47 U.S.C. § 227(b)(1)(A)(iii) (2006).

[25] 47 C.F.R. § 64.1200 (2010).

[26] 15 U.S.C. § 7712(b) (2006).

[27] 47 C.F.R. § 64.3100 (2010).

[28] 47 U.S.C. § 227(b)(3) (2006).

[29] 47 U.S.C. § 227(e) (2006); *see, e.g.*, Stenehjem v. FreeEats.com, Inc., 2006 ND 84, 712 N.W.2d 828.

[30] FTC is vested with primary enforcement authority. 15 U.S.C. § 7706(a) (2006). State attorneys general also have civil enforcement power. 15 U.S.C. § 7706(f)(1). And Internet providers may bring civil actions. 15 U.S.C. § 7706(g). *See generally*, Gordon v. Virtumundo, 575 F.3d 1040, 1048 (2009).

[31] Decisions interpreting 15 U.S.C. § 7707(b) have found no preemption when the state law does not expressly regulate spam. *See, e.g.*, Gordon v. Virtumundo, 575

rested its decision on TCPA. The court held a text message is a call under TCPA, equipment sending the message is prohibited if it has the *capacity* to dial randomly or sequentially, and consent to receive messages from an "affiliate" or "brand" is limited to corporate relationships based on ownership or control.[32] This holding will likely make lawful mobile advertising more difficult for businesses.

A. Text Messages Are Calls Under TCPA

TCPA prohibits "any call . . . using any [ATDS] . . . to any telephone number assigned to . . . a cellular telephone service . . ." unless the recipient gave prior express consent.[33] TCPA does not define "call." *Satterfield* affirmed a 2003 FCC determination that "call" means "both voice calls and text calls to wireless numbers, including, for example, short messages service (SMS) calls . . ."[34] While previous judicial decisions had reached similar conclusions, *Satterfield* is the first opinion to conduct a *Chevron/Mead*[35] analysis determining the

---

F.3d 1040, 1060-64 (2009); Omega World Travel, Inc. v. Mummagraphics, Inc., 469 F.3d 348 (2006) (pre-empting only causes of action for immaterial misrepresentation, not falsity sounding in tort). In other words, CAN-SPAM does not preempt state laws prohibiting "falsity or deception." *See generally* Katherine Wong, *The Future of Spam Litigation After Omega World Travel v. Mummagraphics*, 20 HARV. J.L. & TECH. 459, 469-72 (2007).

[32] *Satterfield*, 569 F.3d at 950; *see generally* The Complex Litigator, In Satterfield v. Simon & Schuster, Inc., Ninth Circuit defers to FCC and construes text messages as "calls" under TCPA, June 22, 2009, http://www.thecomplexlitigator.com/post-data/2009/6/22/in-satterfield-v-simon-schuster-inc-ninth-circuit-defers-to.html (last visited Apr. 22, 2010).

[33] 47 U.S.C. § 227(b) (2006); 47 C.F.R. § 64.1200 (2010).

[34] *In re* Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 18 F.C.C.R. 14014, 14115 ¶ 165, 2003 WL 21517853 (2003) (Report and Order); *see also* Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 19 F.C.C.R. 15927, 15934 (2004) (confirming "prohibition on using [ATDS] to make calls to wireless phone numbers applies to text messages . . . as well as voice calls.").

[35] Chevron, U.S.A., Inc. v. Natural Res. Def. Council, 467 U.S. 837, 842-43 (1984); U.S. v. Mead Corp., 533 U.S. 218, 226-27 (2001); *see generally* Evan J. Criddle, Chevron's *Consensus*, 88 B.U.L. REV. 1271 (2008); William N. Eskridge, Jr.

appropriate level of deference to give the FCC opinion.[36]

Before *Satterfield*, defendants had argued messages sent Internet-to-phone (e-mails converted into text messages) were not calls and therefore CAN-SPAM applied and prevented private lawsuits. For example in *Joffe v. Acacia Mortgage Corp.*, the defendant argued TCPA did not apply because text messages were first e-mailed. But the *Joffe* Court rejected that argument and held TCPA also applies to text messages originally sent by e-mail: "[w]hether a text message is sent phone-to-phone or Internet-to-phone, the end result is the same."[37]

Satterfield affirmed this prohibition on Internet-to-phone messages also applies to text messages sent phone-to-phone. In part, *Satterfield* relied on the FCC's determination that "it is unlawful to make *any call* using an [ATDS] . . . to any wireless telephone number . . . . *This encompasses both voice calls and text calls* to wireless numbers including, for example, short message service . . ."[38] *Joffe* had cited the same FCC order, but had not conducted a *Chevron/Mead* analysis regarding the appropriate level of deference.[39] *Satterfield* is therefore the first decision to do so.

First, *Satterfield* determined Congress intended an ordinary meaning of "to call": "to communicate or try to get into communication with a person by telephone."[40] The court also noted the purpose

---

& Lauren E. Baer, *The Continuum of Deference: Supreme Court Treatment of Agency Statutory Interpretations From* Chevron *to* Hamden, 96 GEO. L.J. 1083 (2008).

[36] Two other decisions have followed *Satterfield* to affirm text messages are calls under TCPA. Abbas v. Selling Source, LLC, No. 09 CV 3413, 2009 WL 4884471 (N.D. Ill. Dec. 14, 2009) (reaching the same conclusion without *Chevron* deference); Lozano v. Twentieth Century Fox Film Corp., No. 09-CV-6344, 2010 WL 1197884 (N.D. Ill Mar. 23, 2010) (deferring to the FCC's 2003 opinion).

[37] Joffe v. Acacia Mortgage Co., 121 P.3d 831, 838 (Ariz. Ct. App. 2005).

[38] Satterfield v. Simon & Schuster, Inc., 569 F.3d 946, 952 (9th Cir. 2009) (citing *In re* Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 18 F.C.C.R. 14014, 14115 (2003)) (emphasis added).

[39] *Joffe*, 121 P.3d at 837 n.6.

[40] *Satterfield*, 569 F.3d at 954 (citing WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 318 (2002)); *accord Joffe*, 121 P.3d at 835 (noting "when the word call is used as a verb, one of its most common meanings is to communicate or try to

of TCPA was to prohibit "communicat[ing] with others by telephone in a manner that would be an invasion of privacy" and "a voice message or a text message are not distinguishable in terms of being an invasion of privacy."[41] Next, the court found the FCC's interpretation of "call" reasonable because it was consistent with the dictionary definition "that text messaging is a form of communication used primarily between telephones."[42] Applying *Chevron*, the court deferred to the FCC's interpretation and therefore held a text message is a "call" under TCPA.[43]

The court's holding, that a text message is a call under TCPA, may increase the likelihood of mobile advertisers being found liable for text-message spam, but those following best practices guidelines should not be significantly affected.[44] In particular, guidelines from MMA already prohibit sending unsolicited messages, require that consumers affirmatively opt-in, and mandate that all messages contain directions on how to opt-out.[45] Moreover, selling mobile opt-in lists is prohibited.[46] In sum, although text messages are now clearly calls, the best practices guidelines are largely consistent with TCPA rules governing such calls for advertising purposes.

---

communicate with by tele-phone."). While other courts have subsequently agreed a "text message" is a "call," the Ninth Circuit's reasoning is somewhat problematic. In particular, the court relied on the *verb* form "to call" ("to communicate with or try to get into communi-cation . . . by a telephone"), but TCPA clearly uses "call" as a *noun*—"It shall be unlawful for any person . . . *to make any call* . . . using any [ATDS] . . ." *Compare Satterfield*, 569 F.3d at 954 *with* 47 U.S.C. § 227(b)(1) (2006) (emphasis added).

[41] *Satterfield*, 569 F.3d at 954.

[42] *Id.*

[43] *Id.*

[44] William B. Baker & Scott D. Delacourt, Important Mobile Marketing Decision by the Ninth Circuit, http://www.wileyrein.com/publications.cfm?sp=articles &id=5271 (last visited Apr. 22, 2010).

[45] *See* GUIDELINES, *supra* note 21, at 13-14, 16.

[46] *Id.* at 16.

B. ATDS Means "Capacity" to Dial Randomly or Sequentially

TCPA prohibits using an ATDS to call any cellular telephone service without express prior consent. *Satterfield* is the first circuit court decision construing the definition of an ATDS under TCPA. Based on the statute's text, the court interpreted ATDS very broadly: "equipment which has the *capacity* to both (1) store or produce numbers to be called using a random or sequential number generator and (2) to dial such numbers."[47]

Such a broad definition poses a serious challenge to mobile advertisers because all computers arguably have the capacity to generate random numbers. Therefore, under *Satterfield*, a large portion of mobile marketers are potentially at risk. In response, advertisers formed the Mobile Advocacy Coalition (MAC) to lobby the FCC to protect underlying technology providers from liability based on *Satterfield's* new definition of ATDS.[48] Although the FCC's 2003 opinion[49] suggested any capacity would be sufficient to render equipment an ATDS, such a broad interpretation might not be

---

[47] *Satterfield*, 569 F.3d at 949 (citing 47 U.S.C. § 227(a)(1) (2006); 47 C.F.R. § 64.1200(f)(1) (2010)) (emphasis added). The district court had held TCPA did not apply because Simon & Schuster's messages were sent to a targeted list of numbers and therefore not randomly generated. But *Satterfield* found the district court had focused on the wrong issue: "[A] system need not actually store, produce, or call randomly or sequentially generated telephone numbers, it need only have the capacity to do it." *Id.* at 951.

[48] Mobile Advocacy Coalition, *Mobile Marketing: What's At Stake & What We're Doing About It*, http://www.mobileac.org/2009/06/mobile-advocacy-coalition.html (June 24, 2009, 1:59 PM EST). MAC plans to petition the FCC for an exemption from liability as "mere conduits" of advertising. This would amount to a finding that the "sender," for TCPA liability purposes, is the user of the mass texting technology rather than the underlying technology provider. There is precedent for such exemptions: the FCC exempted carriers and fax broadcasters from liability as mere conduits. *Cf.* Portuguese Am. Leadership Council of the U.S., Inc. v. Investors' Alert, Inc., 956 A.2d 671 (2008); Lunney v. Prodigy Servs. Co., 94 N.Y.2d 242 (1999).

[49] *In re* Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, 18 F.C.C.R. 14014, 14091-93, 2003 WL 21517853 (2003).

entitled to deference without formal notice-and-comment rulemaking.[50] Nevertheless, MAC's plans are nascent and therefore advertisers who have relied on their equipment not being an ATDS under TCPA should review their practices in light of *Satterfield.*

One issue the Ninth Circuit did not reach was whether the equipment used to send the message to Satterfield actually *dialed* Satterfield's number within the meaning of TCPA. TCPA does not define the word "dial."[51] The *Joffe* court had interpreted "dial" to mean "operate or manipulate a device in order to make or establish a telephone call or connection."[52] *Joffe* therefore concluded sending Internet-to-phone text messages was dialing because "[e]ven though Acacia used an attenuated method to dial a cellular telephone number, it nevertheless did so."[53] Advertisers using computers to send messages might consider raising this issue in an effort to mitigate *Satterfield's* focus on capacity to dial random or sequential numbers.

---

[50] "An agency interpretation must be preceded by some minimum of process to merit deference; simple agency pronouncements, opinion letters, and policy statements fall below that minimum." Abbas v. Selling Source, LLC, No. 09 CV 3413 at *12, 2009 WL 4884471 (N.D. Ill. Dec. 14, 2009) (citing Krzalic v. Republic Title Co., 314 F.3d 875, 881 (7th Cir. 2002)). The FCC's original notice of proposed rulemaking only requested comments "on the various technologies used to dial telephone numbers . . . and whether an autodialer can generate phone calls from a database of existing numbers." *In re* Rules and Regulations Implementing Telephone Consumer Protection Act of 1991, Notice of Proposed Rulemaking and Memorandum Opinion and Order, 17 F.C.C.R. 17459, 17474, 2002 WL 31084939 (Sept. 18, 2002). This notice arguably did *not* request comment on whether *all* systems with capacity to dial randomly or sequentially should be considered an ATDS. Therefore, to the extent the 2003 FCC opinion spoke to this issue, it may have done so without process.

[51] 47 U.S.C. § 227(a)(1)(B) (2006).

[52] Joffe v. Acacia Mortgage Co., 121 P.3d 831, 838 n.10 (2005) (citing WEBSTER'S NINTH COLLEGIATE 349 (1990)) (internal quotations omitted).

[53] *Id.* at 839. For a criticism of this view see J. Wesley Harned, *Telemarketers Gone Mobile: The Telephone Consumer Protection Act of 1991 and Unsolicited Commercial Text Messages*, 97 KY. L. J. 313, 330 (2009) (arguing text messages may not fall under TCPA because sending them does not involve dialing).

C. *"Affiliate" and "Brand" Defined Narrowly by Ownership and Control*

When Satterfield downloaded the ringtone onto her son's cell phone, she consented to receive "promotions from Nextones affiliates and brands."[54] *Satterfield* held that Simon & Schuster was not an "affiliate" or "brand" of Nextones and therefore Satterfield did not consent to the text-message advertising. The court's interpretations of "affiliate" and "brand" impose narrow legal definitions on these terms that undermine the move to jargon-free Web site disclosures.

Simon & Schuster argued the various agreements between Nextones, MIA, and ipsh! permitted advertising to Satterfield. In particular, Nextones had licensed its subscribers' telephone numbers, including Satter-field's, to MIA. MIA then sold the numbers to ipsh!, Simon & Schuster's advertiser.[55] When ipsh! sent the message with the tag line "PwdbyNexton," this was an attempt to label the advertisement as a Nextones message. Simon & Schuster argued it was therefore an affiliate of Nextones and was authorized to send the message:

> Thus, although Nextones shares no corporate structure with [Simon & Schuster] and is not a corporate "affiliate" in a strict legal sense, [Simon & Schuster] submit that the fact that Nextones licensed its subscriber list for use in this campaign constitutes the requisite degree of affiliation . . .[56]

The court rejected this plain reading of "affiliate"—a meaning often employed in online terms and conditions in an effort to simplify language for consumers.[57] Instead, *Satterfield* appears to have imposed

---

[54] Satterfield v. Simon & Schuster, Inc., 569 F.3d 946, 949 (9th Cir. 2009).

[55] *See supra* note 20.

[56] Defendants' Motion for Summary Judgment at 20, Satterfield v. Simon & Schuster, Inc., 2006 U.S. Dist. Ct. Motions 2893, (N.D. Cal. Apr. 2, 2007) (No. 06-2893 CW), 2007 U.S. Dist. Ct. Motions LEXIS 35856.

[57] *See generally* Christina L. Kunz et al., *Click-Through Agreements: Strategies for Avoiding Disputes on Validity of Assent*, 57 BUS. LAW. 401, 410 (2001) (explaining terms should be clear and readable); *accord* FEDERAL TRADE COMMISSION, DOT

technical definitions of "affiliate" and "brand" taken from corporate governance and trademark law.[58]

First, the Ninth Circuit found "[t]he term affiliate carries its own independent legal significance . . . [it] refers to a corporation that is related to another corporation by shareholding or other means of control . . ."[59] The court therefore held Simon & Schuster was not an affiliate of Nextones because Nextones neither owned nor controlled Simon & Schuster.[60] Second, the court imposed an equally technical definition of "brands" as "goods identified as being . . . of a single firm."[61] Satterfield did not consent on this basis either because the text message advertised a Simon & Schuster product, not a Nextones product. Furthermore, adding "PwdbyNexton" to the message did not transform Simon & Schuster into a Nextones affiliate or brand.[62]

The court's decision to impose technical definitions on terms and conditions may seriously restrict future efforts to conduct mobile advertising campaigns.[63] For example, it is unclear how companies

---

COM DISCLOSURES 14 (2000), http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus41.pdf (recommending clear language and syntax and avoiding legalese or technical jargon to make disclosures effective and understandable to consumers); U.S. SECURITIES AND EXCHANGE COMMISSION, A PLAIN ENGLISH HANDBOOK 3 (1998) *available at* http://www.sec.gov/pdf/handbook.pdf.

[58] *See* Goldman, *supra* note 20.

[59] *Satterfield*, 569 F.3d at 955 (quoting Delaware Ins. Guar. Ass'n v. Christiana Care Health Servs., Inc., 892 A.2d 1073, 1077 (Del. 2006) (quoting BLACK'S LAW DICTIONARY 59 (7th ed. 1999))) (internal quotations omitted).

[60] *Satterfield*, 569 F.3d at 955.

[61] *Id.* at 955 (quoting WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 268 (2002)).

[62] *Id.* ("Nextones's only role in this case was simply supplying the numbers to MIA, who in turn supplied the numbers to ipsh! The record also shows no agreement between Nextones and Simon & Schuster.").

[63] Ronnie London, *Has The 9th Circuit Raised The Bar For Text-Message Affiliate Marketing?* PRIVACY & SECURITY LAW BLOG, June 24, 2009, http://www.privsecblog.com/2009/06/articles/main-topics/marketing-consumer-privacy/has-the-9th-circuit-raised-the-bar-for-textmessage-affiliate-marketing/ (last visited Apr. 10, 2010). For criticism of the lack of uniformity in privacy policies see Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws* 9 ALB. L.J. SCI. & TECH. 91, 124-33 (2009)

should now identify a third party on their Web site who markets to their customers; describing third parties as "affiliates" will no longer suffice. Moreover, companies can no longer insulate themselves from TCPA liability by stamping messages with the signature of the company that obtained the customer's consent.[64]

This decision also raises significant questions as to what constitutes adequate consent to receive messages. Under MMA best practices, Nextones would have been responsible for collecting user consent to receive promotions, and MIA would have been responsible for using that data in accordance with MMA guidelines.[65] These guidelines for affiliate marketing would also have required Simon & Schuster be identified in the message and in opt-out language.[66] It remains unclear, however, whether such disclosures are still sufficient after *Satterfield.*

CONCLUSION

Satterfield held unsolicited text messages sent by an ATDS are unlawful under TCPA because: (1) text messages are calls; (2) the system sending the messages is an ATDS if it has the capacity to generate numbers randomly or sequentially; and (3) the terms "affiliate" and "brand," when used in online terms and conditions, are defined narrowly.

The court's definition of an ATDS presents a serious challenge to advertisers because all computers arguably have the capacity to generate random numbers. Furthermore, the decision's narrow, technical definitions of "affiliate" and "brand" are troublesome because they may discourage plain language in online terms and conditions and make it difficult for future companies to hire third-party marketing

---

(exploring collection and dissemination of personal identifying information and determining there is little regulation of online privacy policies).

[64] London, *supra* note 63.

[65] Defendants' Motion for Summary Judgment at 20, Satterfield v. Simon & Schuster, Inc., 2006 U.S. Dist. Ct. Motions 2893, (N.D. Cal. Apr. 2, 2007) (No. 06-2893 CW), 2007 U.S. Dist. Ct. Motions LEXIS 35856; GUIDELINES, *supra* note 21.

[66] GUIDELINES, *supra* note 21.

companies. Marketers using third-party lists of telephone numbers must therefore continue to obtain the appropriate warranties, covenants, and indemnity provisions regarding how the numbers were collected, whether the third party is permitted to disclose the numbers, and the ability of marketers obtaining those numbers to use them. And companies hiring third-party marketing companies must ensure the customers who opted-in actually consented to receive text messages.

PRACTICE POINTERS

- When seeking consent from customers, ensure terms and conditions identify exactly what the customer will receive and who will send it. Eschew the use of any terms that have vague or ambiguous meanings such as "brand" or "affiliate" in favor of more precise terms such as "third parties."
- Do not send text messages to customers who did not expressly consent to receive messages.
- Identify all companies that have access to a customer's phone number and ensure each has complied with any restrictions on the customer's express consent.
- Vendors providing lists of phone numbers to marketers that will use the numbers to send text messages should ensure appropriate contractual terms and conditions govern the marketers' uses.
- Marketers that obtain phone numbers from vendors should negotiate appropriate representations, warranties, and indemnities regarding the scope of consent that vendors obtained from consumers.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 6, ISSUE 1 SUMMER 2010

COMMUNICATIONS DECENCY ACT PROVIDES NO SAFE HARBOR AGAINST ANTIFRAUD LIABILITY FOR HYPERLINKS TO THIRD-PARTY CONTENT UNDER THE SECURITIES AND EXCHANGE ACT

Sheri Wardwell[*]

CITE AS: 6 WASH J.L. TECH. & ARTS 49 (2010)
https://digital.lib.washington.edu/dspace-law/handle/1773.1/451

ABSTRACT

In 2008, the U.S. Securities and Exchange Commission (SEC) released interpretive guidelines regarding antifraud liability for statements and disclosures made on company Web sites. The SEC noted that a company may incur both criminal and civil liability under section 10(b) of the Securities Exchange Act and Rule 10b-5 for hyperlinks to third-party content. However, the Communications Decency Act, 47 U.S.C. § 230(c), expressly preempts civil liability for interactive computer service providers that post hyperlinks to third-party content on their Web sites. This Article examines whether section 230 immunizes companies from civil liability for hyperlinks to third-party content despite the SEC's interpretive guidelines imposing antifraud liability. This Article concludes that companies would likely be considered information content providers under section 230 and therefore outside the scope of the safe harbor provision for interactive computer service providers.

---

[*] Sheri Wardwell, University of Washington School of Law, Class of 2010. Thank you Professor Jane K. Winn of the University of Washington School of Law for offering valuable feedback. Also, thank you to James Evans, of Fenwick & West LLP, for his thoughtful review of this Article.

TABLE OF CONTENTS

INTRODUCTION

In response to rapidly expanding Internet use, the U.S. Securities and Exchange Commission (SEC) has increasingly recognized the advantage of having issuers of securities publish company communications, statements, and reports on company Web sites.[1] SEC

[1] *See, e.g.*, Securities Offering Reform, Securities Act Release No. 8591, Exchange Act Release No. 52,056, Investment Company Act Release No. 26,993, 2005 WL 1692642 (Aug. 3, 2005) [hereinafter 2005 Release]; Use of Electronic Media, Securities Act Release No. 7856, Exchange Act Release No. 42,728, Investment Company Act Release No. 24,426, 2000 WL 502290 (April 28, 2000)

guidelines released since 1995 detail a trend towards not only greater acceptance of the Internet as an efficient means for fulfilling disclosure requirements of the Securities Act ('33 Act) and the Securities and Exchange Act ('34 Act),[2] but also increased regulation of company disclosures online.[3] In the 2008 Commission Guidance on the Use of Company Web Sites (Guidelines), the SEC clarified its position of imposing liability for communications, statements, and reports published on company Web sites.[4] To protect investors from misleading hyperlinked content on company Web sites, section 10(b) of the '34 Act and Rule 10b-5[5] impose civil liability for hyperlinked third-party content containing a material misstatement or omission that is attributable to the company.[6]

[hereinafter 2000 Release]; Use of Electronic Media for Delivery Purposes, Securities Act Release No. 7233, Exchange Act Release No. 36,345, Investment Company Act Release No. 21,399, 60 Fed. Reg. 53,458 (Oct. 13, 1995) [hereinafter 1995 Release].

[2] For instance, issuers are now encouraged to make prospectuses (2005 Release), annual reports (2000 Release), proxy materials (2000 Release), and Regulation FD disclosures (2008 Release) available online.

[3] For example, when a company is in registration, communication on the company's Web site—including hyperlinked information—that meets the definition of an "offer to sell," "offer for sale" or "offer" under section 2(a)(3) of the '33 Act is subject to liability under section 5 of the '33 Act. 2000 Release, *supra* note 1. In the 2000 Release the SEC requested comment on whether a company may be liable for communications made by or on behalf of a company on electronic forums, including blogs. In 2008, liability for communications was expanded to communications on electronic forums. Commission Guidance on the Use of Company Web Sites, Exchange Act Release No. 58,288, Investment Company Act Release No. 28,351, 2008 WL 4068202, (Aug. 7, 2008), *available at* http://www.sec.gov/rules/interp/2008/34-58288.pdf.

[4] Commission Guidance on the Use of Company Web Sites, Exchange Act Release No. 58,288, Investment Company Act Release No. 28,351, 2008 WL 4068202 (Aug. 7, 2008) [hereinafter 2008 Release], *available at* http://www.sec.gov/rules/interp/2008/34-58288.pdf.

[5] 15 U.S.C. § 78j(b) (2006), *available at* http://www.law.cornell.edu/uscode/15/usc_sec_15_00000078---j000-.html; 17 C.F.R. § 240.10b-5, *available at* http://www.law.uc.edu/CCL/34ActRls/rule10b-5.html.

[6] 2008 Release, *supra* note 4. While this Article discusses liability for hyperlinks under section 10(b) of the '34 Act, a company may also be liable under provisions of the '33 Act and the '34 Act for hyperlinks to third-party content, such as section

Section 230 of the Communications Decency Act provides a safe harbor for interactive computer service providers by preempting liability for publishing third-party content.[7] If section 230 preempts antifraud liability under the '34 Act, a company would be immunized from civil liability.[8] However, a company's antifraud liability for hyperlinks to third-party content under the '34 Act appears to be outside the scope of the section 230 safe harbor for interactive computer service providers. This Article examines (1) the nature of the SEC's Guidelines regarding liability for hyperlinks to third-party information under the Securities and Exchange Act and (2) whether section 230 can immunize a company from antifraud liability described in the Guidelines for hyperlinks to third-party content.

I. SEC GUIDELINES IMPOSE LIABILITY ON COMPANIES HYPERLINKING TO THIRD-PARTY CONTENT TO PROTECT INVESTORS

According to the SEC's interpretive releases on the use of company Web sites, companies are responsible for statements that may "reasonably be expected to reach investors or the securities markets

---

17(a) of the '33 Act for fraudulent sales or offers to sell securities.

[7] 47 U.S.C. § 230 (2006), *available at* http://www4.law.cornell.edu/uscode/47/230.html.

[8] *See* Eric Goldman, *SEC's Proposed Guidance on Hyperlinking Contravenes 47 USC 230*, TECHNOLOGY & MARKETING LAW BLOG, Nov. 05, 2008, http://blog.ericgoldman.org/archives/2008/11/secs_proposed_g.htm (arguing "§ 230 preempts all civil causes of action based on third party online content – even causes of action enforced by the SEC."); Eric Goldman, *SEC Proposes that Companies Should Be Liable for Content Linked From the Company's Web site*, TECHNOLOGY & MARKETING LAW BLOG, Aug. 28, 2008, http://blog.ericgoldman.org/archives/2008/08/sec_proposes_th.htm (noting section 230 may provide a defense against fraudulent marketing under the '34 Act); Eric Goldman, *Do the FTC's New Endorsement/Testimonial Rules Violate 47 USC 230?*, TECHNOLOGY & MARKETING LAW BLOG, Oct. 06, 2009, http://blog.ericgoldman.org/archives/2009/10/do_the_ftcs_new.htm (analogizing prior arguments made against the SEC to the Federal Trade Commission's imposition of liability for advertisers linking to misleading endorsements under the Federal Trade Commission guidelines codified in 16 C.F.R. § 255).

regardless of the medium through which the statements are made, including the Internet."[9] Because of the widespread use of the Internet amongst investors, any online content attributed to a company can reasonably be expected to reach investors. Liability not only extends to communications made by or on behalf of a company on Web sites, blogs, or forums, but may also extend to hyperlinked content of third parties, such as reports made by financial analysts embedded on a company Web site that can be attributed to that company.[10] A private cause of action may be brought against a company for hyperlinked content under section 10(b) of the '34 Act and Rule 10b-5 when the hyperlinked content can be attributed to the company and the hyperlink creates a material misstatement or omission in connection with the sale or purchase of the company's securities.[11]

The SEC considers hyperlinked content embedded on a company's Web site attributable to that company when the company has either entangled itself in the preparation of the information or adopted the information.[12] Under the entanglement theory, third-party content is attributable to a company when the company was involved in the preparation of the information.[13] For instance, a company may be

---

[9] 2000 Release, *supra* note 1, § (II)(B); *see also* 2008 Release, *supra* note 5.

[10] 2008 Release, *supra* note 4, §§ II(B)(2),(4). *See generally* Robert A. Prentice, Vernon J. Richardson, & Susan Scholz, *Corporate Web Site Disclosure and Rule 10B-5: An Empirical Evaluation*, 36 AM. BUS. L.J. 531 (1999) (examining the various mechanisms by which a company can be held liable under Rule 10b-5).

[11] 2008 Release, supra note 4; *see also* 15 U.S.C. § 78j(b) (2006), *available at* http://www.law.cornell.edu/uscode/15/usc_sec_15_00000078---j000-.html; 17 C.F.R. § 240.10b-5, *available at* http://www.law.uc.edu/CCL/34ActRls/rule10b-5.html.

[12] 2000 Release, *supra* note 1, § II(B)(1).

[13] *Id. See also In re* Presstek, Inc., Exchange Act Release No. 997, 66 SEC Docket 328, § III(C)(3)(a) (Dec. 22, 1997) (holding issuers liable for false statements by others made in a research report if the issuer has "sufficiently entangled itself" with the content. (quoting Elkind v. Liggett & Myers, Inc., 635 F.2d 156, 163 (2d Cir. 1980))). *In re Presstek* indicates that proof of an issuers involvement in the preparation is necessary, but notes *Eisenstadt v. Allen*, 113 F.3d 1240, 1997 WL 211313 (9th Cir. 1997) (unpublished table decision), leaving the door open for post-preparation involvement to be sufficient to attribute content to the issuer. *Id.*

entangled if its activity suggests an implied representation that the third-party content was reviewed and is in accordance with the company's views.[14]

Under the adoption theory, the content is attributable to the company if the company either "explicitly or implicitly endorsed or approved the information" regardless of whether the company was involved in the preparation of the content.[15] A company is presumed to have implicitly adopted information when it includes a hyperlink within a report that must be filed pursuant to federal securities laws.[16] However, when hyperlinks are used, for example, on a company Web site, the circumstances surrounding the use of the hyperlinks must be considered to determine whether the hyperlinked content should be implicitly attributed to a company.[17] In general, providing a link to third-party content indicates a company's belief that "the information on the third-party website may be of interest to the users of its website."[18]

To avoid the attribution of hyperlinked content, a company may use disclaimers, intermediary screens explaining why the link was provided, or exit notices between the company's Web site and the third-party's Web site.[19] However, no single tactic immunizes a company from attribution of content under the adoption theory.[20] Ultimately, adoption of content is determined by examining whether there

---

[14] Elkind v. Liggett & Myers, Inc., 635 F.2d 156, 163 (2d Cir. 1980).

[15] 2000 Release, *supra* note 1, § II(B)(1).

[16] *Id.*

[17] 2008 Release, *supra* note 4, § II(B)(2) (for instance, the SEC notes that a company's statements about the hyperlink, the risk of confusion for investors, precautions taken to warn investors, and the presentation of the hyperlinked information on the Web site should inform a company as to whether a hyperlink will be attributable).

[18] *Id.*

[19] *Id. See also* Mason Miller, *Technoliability: Corporate Websites, Hyperlinks, and Rule 10(b)-5*, 58 WASH. & LEE L. REV. 367, 395 (2001) (discussing use of disclaimers accompanying hyperlinks to fall within the safe harbor for forward-looking statements codified in the 1995 Private Securities Litigation Reform Act).

[20] *Id.* Of note, waivers of liability under the '34 Act are ineffective. 15 USC § 78cc (2006).

is a reasonable inference that the company endorsed or approved the content.[21]

II. SAFE HARBOR UNDER SECTION 230 DOES NOT IMMUNIZE COMPANIES FROM LIABILITY UNDER SECTION 10(B) OF THE '34 ACT AND RULE 10B-5

Section 230(c) of the Communication Decency Act (CDA) is generally understood to immunize interactive computer service providers (service providers) from civil liability for state and federal claims regarding third-party content published on their Web site.[22] It has been suggested that section 230 may immunize a company that violated section 10(b) of the '34 Act and Rule 10b-5 by hyperlinking from the company Web site to third-party content.[23] However, section 230 cannot preempt antifraud liability under section 10(b) of the '34 Act and Rule 10b-5 when the section 230 safe harbor can be harmonized with the SEC's imposition of liability under the Guidelines and there is no conflict between the two rules.[24] Because companies that have

---

[21] *Id.*

[22] 47 U.S.C. § 230(c) (2006), *available at* http://www4.law.cornell.edu/uscode/47/230.html. A service provider can be immunized from a variety of claims under the section 230 safe harbor. *See* Doe v. MySpace, Inc., 528 F.3d 413, 418 (5th Cir. 2008) (stating that "courts have construed the immunity provisions in section 230 broadly in all cases arising from the publication of user-generated content."); Jonathan Band & Matthew Schruers, *Safe Harbors Against the Liability Hurricane: The Communications Decency Act and the Digital Millennium Copyright Act*, 20 CARDOZO ARTS & ENT. L.J. 295, 297-98 (2002) (describing the broad application of the section 230 safe harbor to various state law claims ranging from negligence to infliction of emotional distress).

[23] *See, e.g.*, Eric Goldman, *SEC's Proposed Guidance on Hyperlinking Contravenes 47 USC 230*, TECHNOLOGY & MARKETING LAW BLOG, Nov. 05, 2008 http://blog.ericgoldman.org/archives/2008/11/secs_proposed_g.htm. Goldman suggests that section 230 preempts antifraud liability. However, if section 230 and the imposition of liability under section 10(b) of the '34 Act and Rule 10b-5 are not in conflict because antifraud liability for a company is outside the scope of the section 230 safe harbor, section 230 cannot preempt antifraud liability.

[24] The canon of harmonization requires a court to reconcile conflicting statutes where possible so that each is effective in its purpose. *See* Timothy K. Armstrong,

adopted third-party content, or participated in its preparation, appear to be outside the intended, apparent, and judicially interpreted scope of section 230 safe harbor for service providers, the rules are not in conflict and section 230 cannot be used as an affirmative defense to a section 10(b) of the '34 Act and Rule 10b-5 violation.

A. The Congressional Intent of Section 230 Indicates that Company Liability Under the '34 Act is Outside the Scope of Safe Harbor

The CDA was promulgated to prevent exposure of objectionable and indecent materials to minors.[25] Congress recognized that while service providers may be able to limit the quantity of objectionable and indecent materials online, the service providers could not possibly regulate all materials posted by third parties. Because Congress feared the threat of tort liability would decrease incentives for service providers to continue contributing to the growth of the Internet,[26] section 230 was added to immunize service providers who blocked or screened objectionable material[27] by providing that service providers shall not be held liable on account of self-regulatory activity and "shall not be treated as the publisher or speaker of any information provided

---

Chevron Deference and Agency Self-Interest, 13 CORNELL J.L. & PUB. POL'Y 203, FN 341 (2004) (describing the role of the judiciary to harmonize apparently conflicting statutes when possible). *But see* Karl N. Llewellyn, *Remarks on the Theory of Appellate Decision and the Rules or Canons About How Statutes Are To Be Construed*, 3 VAND. L. REV. 395, 401-06 (1950) (noting that there are number of applicable canons, many of which may be paradoxically applied, and their ultimate usefulness is heavily influenced by the desired outcome).

[25] *See* Communications Decency Act of 1996, Pub. L. No. 104-104, Title V § 230 (1996).

[26] Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997), *cert. denied*, 118 S. Ct. 2341 (1998). *See also* 47 U.S.C. § 230(b) (affirming "It is the policy of the United States . . . to promote the continued development of the Internet and other interactive computer services and other interactive media . . .").

[27] H.R. Rep. No. 104-458, at 194 (1996) (where the House of Representatives amendment, later codified as section 230, is intended to "protect[ ] from civil liability those providers and users of interactive computer services for actions to restrict or to enable restriction of access to objectionable online material.").

by another information content provider."[28]

By enacting section 230, Congress specifically intended to overrule decisions such as *Stratton Oakmont v. Prodigy Services*, which imposed liability on service providers for third-party content.[29] In *Stratton*, Prodigy Services was a service provider of an online bulletin holding itself out to the public as controlling the content of messages posted by third parties.[30] When the service provider did not either edit or remove unlawful content, the service provider was found liable as a publisher of unlawful third-party content despite the service provider's arguments that it was impossible to patrol all of the content posted to the bulletin.[31] Section 230 specifically overturned *Stratton* by precluding the imposition of publisher liability on a service provider for editing or regulating third-party content.

The legislative record does not indicate blanket immunity for all service providers under section 230. Rather, section 230 safe harbor appears to be restricted to those service providers, such as Prodigy Services, that are not claiming the content as their own but rather are acting merely as conduits or editors of material posted by third parties. Companies liable under the '34 Act for hyperlinks to third-party content are more than mere service providers, such as Prodigy Services, that may or may not edit third-party content. Such companies deliberately place hyperlinks to third-party content because they have determined that the information is useful and intend Web site visitors to read and consider the content. Companies that post content to further a Web site visitor's understanding of the company are readily distinguishable from companies, such as Prodigy Services, offering a forum by which third parties can choose to post their own content. As such, a company liable under the '34 Act appears to be outside the intended scope of the section 230 safe harbor.

---

[28] 47 U.S.C. § 230(c) (2006).

[29] H.R. Rep. No. 104-458, at 194 (1996) (citing Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. Ct. 1995) (unpublished opinion)).

[30] Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. Ct. 1995) (unpublished opinion).

[31] *Id.*

Further, the SEC's goal of protecting investors from being misled in the securities market by holding companies liable for hyperlinked information is consistent with Congress's intent that section 230 only provide safe harbor for service providers acting as mere conduits of third-party content on the Internet. Precluding companies from invoking the section 230 safe harbor for conduct impermissible under the '34 Act would not have the detrimental effect on the growth of the Internet Congress sought to avoid. In fact, the SEC anticipates increasing use of the Internet by companies seeking to communicate with investors.[32]

B. The Plain Meaning of Section 230 Indicates that Companies Liable Under the '34 Act are Outside the Scope of Safe Harbor

The plain meaning of section 230(c) broadly grants federal immunity against all civil causes of action.[33] The only significant limitation to section 230(c) is that safe harbor only applies to service providers, not information content providers (content providers).[34] A service provider is "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."[35] By contrast, a content provider is "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[36] While service providers act as a conduit for posting information, content providers have played some role in creating or developing the information posted online. Because section 230(c)(1) immunizes only

---

[32] *See supra* note 7.

[33] § 230(e). *See also*, Band & Schruers, *supra* note 22.

[34] § 230(c)(1) (stating, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

[35] § 230(f)(2).

[36] § 230(f)(3).

service providers, any content provider that contributed to the objectionable content remains subject to civil liability for content posted online.[37]

A company that maintains a company Web site is likely a content provider and not a service provider in situations where antifraud liability under the '34 Act is at issue. The SEC requires that third-party content be attributable to a company for the company to incur liability under the '34 Act. Under the entanglement theory, information is attributed to a company if the company was responsible for the preparation of the information.[38] Content providers meet the attribution definition under entanglement theory because they are responsible for the preparation of information or have participated, in whole or in part, in the "creation or development" of the information. Therefore, demonstration that a company is entangled with the hyperlinked information may also demonstrate that a company is a content provider and outside the bounds of safe harbor protection under section 230.

C. *The Judicial Interpretation of Section 230 Indicates that Companies Liable Under the '34 Act are Outside the Scope of Safe Harbor*

Courts are generally cautious about extending the scope of safe harbor under section 230 and will often try to balance the seemingly narrow congressional intent of section 230 against the apparently broad grant of immunity in section 230(c)(1).[39] Ultimately, the scope of section 230 is determined by whether the provider is considered a

---

[37] *See* Carafano v. Metrosplash.com. Inc., 339 F.3d 1119, 1125 (9th Cir. 2003) (where soliciting data through an online questionnaire did not constitute "a significant role in creating, developing or 'transforming' the relevant information" and therefore the online dating service was not an internet content provider under 47 U.S.C. § 230(f)(3)).

[38] *See supra* note 13.

[39] *See Carafano*, 339 F.3d at 1122-23 (refusing to expand section 230 so broadly as to create an advantage for online businesses over businesses operating in the "real world"); Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 669 (7th Cir. 2008).

service provider or content provider.[40] The clearest example of service providers with immunity under the section 230 safe harbor are generally Web sites, like eBay, Google and AOL, that publish content volunteered by third parties.[41] The mantra appears to be that a passive provider is a safe provider. However, the distinction between a service provider that merely publishes another's content and a content provider that creates and develops content is not clear, especially when a provider can operate within both spheres.[42] To resolve the distinction, courts have largely relied on the extent of the contribution to the creation or development of the content and the extent to which the provider is the "publisher or speaker" of the content.

1. Contribution to the Creation or Development of Content

When a provider is merely a conduit for information and provides no editorial contribution—similar to a telephone company relaying signals between two customers—safe harbor under section 230 is permissible.[43] For example, in *Zeran v. America Online* the Fourth

---

[40] Zeran v. Am. Online, Inc., 129 F.3d 327, 327 (4th Cir. 1997) (establishing that section 230 immunity depends on whether the provider is an interactive computer service provider and not an information content provider).

[41] *See* Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 714-15 (Cal. Dist. Ct. App. 2002) (provider of online marketplace is an internet service provider); Parker v. Google, 422 F.Supp.2d 492, 500-01 (E.D. Pa. 2006) (stating "there is no doubt that Google qualifies as an 'interactive computer service'" eligible for immunity under section 230); Ben Ezra, Weinstein, & Co. v. Am. Online Inc., 206 F.3d 980, 985 (10th Cir. 2000) (provider of e-mail service is an interactive computer service provider).

[42] *See, e.g.,* Mazur v. eBay, No. 07-03967, 2008 WL 618988 (N.D. Cal. July 23, 2008), *available at* http://scholar.google.com/scholar_case?case=7015046710981364619&hl=en&as_sdt=2&as_vis=1&oi=scholarr (defining eBay as an interactive computer service provider with immunity under section 230 when eBay failed to withdraw third-party content it knew to be illegal, but noting that eBay can function as both an interactive computer service provider as well as an information content provider).

[43] *See Ben Ezra*, 206 F.3d at 986 (holding America Online immune from liability for publishing inaccurate stock information by third parties because the contract between America Online and the third parties provided that AOL "may not modify,

Circuit held America Online not liable for inappropriate content posted to its message board by a third party when America Online merely provided the message board service and was not involved in either creating the content or encouraging third parties to post such content.[44]

However, a provider who makes a material editorial contribution, beyond merely transmitting a third party's content or making minor edits, will be considered to have participated in the "creation or development" of content under section 230 and will not be eligible for safe harbor.[45] In *Fair Housing Council v. Roommates.com*, a roommate-matching Web site was considered a content provider, unable to claim section 230 immunity, because it was considered the developer of infringing content when it created a questionnaire and required users to answer questions that violated the Fair Housing Act.[46] Even though the Roommates.com users ultimately made the selections using a drop-down menu in the questionnaire, Roommates.com was liable as a content provider because it created a questionnaire where the users had no choice but to violate the Fair Housing Act.[47] The court determined that "development" is defined as "making usable or

---

revise, or change" the information it received from the third parties. America Online was therefore contractually prohibited from being a content provider); Universal Commc'n Sys., Inc. v. Lycos, 478 F.3 d 413, 420 (1st Cir. 2007) (determining that a message board operator is protected under section 230 for postings by third parties, even when the message board operator knew that the content was illegal, when the message board operation was not involved in the creation or development of the content).

[44] *Zeran*, 129 F.3d at 330.

[45] *See* Hy Cite Corp. v. badbusinessbureau.com, LLC, 418 F.Supp.2d 1142, 1149 (D. Ariz. 2005) (denying CDA immunity to a provider that contributes content and solicits third-party content for a newsletter even though the provider did not contribute to the creation of the newsletter's unlawful content); Blumenthal v. Drudge, 992 F. Supp. 44, 50 (D.D.C. 1998) (holding a publishing of a gossip column immune from liability as a service provider, but indicated that section 230 would not immunize the creator of the gossip column because such a creator is an information content provider).

[46] Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008) (en banc).

[47] *Id.* at 1172.

available" or "the process of researching, writing, gathering, organizing and editing information for publication on web sites."[48] If Roommates.com had merely created an open-ended questionnaire, where users had a choice whether or not to provide infringing content, section 230 safe harbor may have been appropriate because Roommates.com would not have contributed to the "development" of the infringing content by either writing, gathering, organizing or editing the user provided information.[49] While a service provider may offer traditional editorial input without such input being considered a contribution to the creation or development of content,[50] a provider that induces the unlawful content or impermissibly selects content for publication will be considered a content provider and outside the scope of the section 230 safe harbor.[51]

---

[48] *Id.* at 1168 (citing WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY for the definition of "develop" and WIKIPEDIA for the definition of "web content development").

[49] *See* Carafano v. Metrosplash.com. Inc., 339 F.3d 1119, 1125 (9th Cir. 2003) (soliciting data from an open-ended questionnaire where users filled in blank space did not constitute "a significant role in creating, developing or 'transforming' the relevant information" because the users had a choice whether to provide infringing content and, therefore, the online dating service was not a content provider. In contrast to *Roommates.com*, the court considered the answers unlawful, not the questionnaire).

[50] Mazur v. eBay, No. 07-03967, 2008 WL 618988 (N.D. Cal. July 23, 2008) (deciding whether to publish is a traditional editorial function that is acceptable for an internet service provider seeking safe harbor under section 230). See also Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003) (determining that a defendant was not an information content provider of an e-mail when he made minor alterations to a tortious e-mail provided by a third party to include in a newsletter); Doe v. Friendfinder Network, Inc, 540 F.Supp.2d 288 (D.N.H. 2008) (finding that a provider who re-posted a profile on a social networking site with "slight" modifications that did not contribute to the injurious character of the posting was immune from state law causes of action).

[51] Fair Hous. Council, 521 F.3d at 1166-69 (a service provider cannot claim safe harbor if it "contributes materially to the alleged illegality of the conduct," such as when it requests users to supply discriminatory criteria or uses the unlawful criteria to limit information that users can access). Compare NPS LLC v. StubHub, Inc., No. 06-4874-BLS1, 2009 WL 995483 (Mass. Super. Ct. Jan. 26, 2009) (citing Fair Housing Council to bar StubHub from claiming section 230 immunity when it

Under current jurisprudence, a court would likely characterize a company, liable under the '34 Act for hyperlinking to third party content, as a content provider. In particular, posting hyperlinks is an editorial function and clearly "creation or development."[52] The judiciary has refused to immunize service providers that have either contributed more than traditional edits to the content[53] or contributed materially to the development of the third-party content.[54] Under the entanglement theory of attribution, an issuer can only be liable under the securities laws when the issuer has so involved itself in the preparation of the information that the content can be attributed to the issuer.[55] Such preparation involves more than mere editing or providing a conduit by which third parties may pass along information. Rather, in order for information to be attributed to a company, the company must have aided in the development or creation of the content; by implication, this content is deemed to represent the company's views.

Like in *Fair Housing Council*, a company liable under the '34 Act for fraudulent hyperlinks is more than a "passive transmitter" when it contributes, at least in part, to the development of infringing content by researching, gathering, and making the third-party content available on its Web site. Because the entanglement theory has substantial requirements for the content to be attributed to a company, a company that is found liable under section 10(b) of the '34 Act and Rule 10b-5 may also be considered a content provider and, therefore, ineligible for the section 230 safe harbor.

"materially contributed to the illegal 'ticket scalping' of its sellers" by allowing ticket scalpers to resale tickets in a way that blocked the identify of the resellers and purchasers), with Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 671 (7th Cir. 2008) (finding that Craigslist was immune as a service provider because Craigslist did not "induce[] anyone to post any particular listing or express a preference for discrimination.").

[52] *See supra* text accompanying note 45.

[53] Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).

[54] *Fair Hous. Council*, 521 F.3d at 1167-68.

[55] *See supra* text accompanying note 13.

2. Provider as Publisher or Speaker of Content

In addition to considering the extent of editorial contribution, courts have also weighed the extent to which a provider is said to be a publisher or speaker of third-party content when distinguishing a content provider from a service provider.[56] In *Anthony v. Yahoo!*, Yahoo sent profiles of former subscribers of its dating service to current subscribers in order to mislead and induce current subscribers to continue subscribing.[57] While the profiles were created by third parties, Yahoo was considered a "publisher or speaker" of the profiles when it intentionally misrepresented the profiles to current subscribers of the dating service.[58] Because Yahoo was considered the "publisher or speaker" of the misrepresented profiles, Yahoo was considered a content provider and was barred from using the section 230 safe harbor as a defense for its tortious actions.[59]

A company found liable for violating the '34 Act would likely be considered a content provider and outside the scope of the section 230 safe harbor pursuant to the holding in *Anthony*. Just as Yahoo was considered a content provider when it used former-subscriber profiles to perpetrate a fraud or misrepresentation, a company liable under the '34 Act would be a content provider when the company uses hyperlinks to misrepresent material information to investors.[60] Under the adoption theory, attribution is presumed when a company

---

[56] Anthony v. Yahoo! Inc., 421 F. Supp. 2d 1257 (N.D. Cal. 2006); Batzel v. Smith, 333 F.3d 1033 (9th Cir. 2003) (noting that if the "information is provided to those individuals in a capacity unrelated to their function as a provider or user of interactive computer services, then there is no reason to protect them with special statutory immunity.").

[57] *Anthony*, 421 F. Supp. 2d at 1259-60.

[58] *Id.* at 1263. The court also considered Yahoo an information content provider when it created false profiles to send to subscribers because Yahoo was entirely responsible for the creation or development of such content.

[59] *Id.*

[60] Of note, in both situations, the profiles used by Yahoo or the third-party information used by a company are not themselves unlawful, it is the use of the content by Yahoo or a company that is impermissible.

intentionally hyperlinks to third-party content unless the circumstances surrounding the use of the hyperlink, such as the presence of a disclaimer, would lead a reasonable investor to understand that the company has not adopted the hyperlinked content.[61] Therefore, a company that implicitly adopts third-party content may also be considered a content provider under section 230 because the company is necessarily using third-party content to misrepresent information to investors and perpetrate a fraud under the '34 Act.

Regardless of whether content is attributable to a company under the entanglement theory or the adoption theory, a company liable under the '34 Act for hyperlinking to fraudulent third-party content will likely be considered a content provider because the company is (1) aiding in the creation or development of the content, as distinguished from providing minor editorial contributions like in *Zeran*; (2) contributing to the development of the infringing content by researching, gathering, and making available infringing third-party content on its Web site like in *Fair Housing Council*; or (3) using the third-party content to perpetrate a fraud or misrepresentation like in *Anthony*.

CONCLUSION

Because the SEC's Guidelines indicate that company liability under section 10(b) of the '34 Act and Rule 10b-5 for hyperlinked third-party content require the hyperlinked content be attributable to a company, a company would likely be considered an information content provider under section 230 and outside the scope of the section 230 safe harbor for interactive computer service providers. As such, section 230 safe harbor may not immunize a company from a section 10(b) of the '34 Act and Rule 10b-5 violation.

---

[61] *See supra* text accompanying note 13.

PRACTICE POINTERS

- To avoid the possibility of liability, companies that post statements, disclosures, and reports on their Web sites should protect themselves as if they could be held liable under section 10(b) of the Exchange Act and Rule 10b-5 for embedded hyperlinks to fraudulent third-party content.
- A company that embeds hyperlinks to third-party content on its Web site may avoid antifraud liability by using disclaimers, intermediary screens, exit notices between the issuer's Web site and the third party's Web site, or explanations of why the links were provided to ensure that the content is not attributed to the company.
- Because 47 U.S.C. § 230 can be harmonized with the SEC's Guidelines on antifraud liability for information on company Web sites, section 230 safe harbor is likely a poor defense against private causes of action for fraudulent misstatements or omissions involved in the sale or purchase of securities under section 10(b) of the Exchange Act and Rule 10b-5.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 6, ISSUE 1 SUMMER 2010

STEVENS V. PUBLICIS: THE RISE OF "NO E-MAIL MODIFICATION" CLAUSES?

Stephanie Holmes[*]

CITE AS: 6 WASH J.L. TECH. & ARTS 67 (2010)
https://digital.lib.washington.edu/dspace-law/handle/1773.1/449

ABSTRACT

E-mails occupy an ambiguous space between informal oral conversation and formal written documents. Their legal significance in contract modification is, however, becoming increasingly clear. In April 2008, the Supreme Court of New York, Appellate Division, decided Stevens v. Publicis, S.A. and in the process, raised the legal status of e-mail exchanges in the context of contract modification. Before Stevens v. Publicis, S.A., an e-mail could constitute a "signed writing" under New York law, thus satisfying the statute of frauds. An e-mail exchange could also amend a contract if, for instance, it had been validated by the parties' reliance on it. After Stevens v. Pulicis, S.A., e-mails may also satisfy a "no-oral-modification" (NOM) clause–the contractual obligation to memorialize contract modifications in written and signed documents–without requiring additional contractual validation. This Article discusses the legal underpinnings of this decision and offers practical guidance for attorneys attempting to avoid contract modification by e-mail.

---

[*] Stephanie Holmes, University of Washington School of Law, Class of 2010. Thank you to Elaine D. Ziff of Skadden, Arps, Slate, Meagher & Flom LLP for her invaluable insight and guidance. Many thanks also to Professor Jane K. Winn of the University of Washington School of Law and Chelsea Peters, student editor.

TABLE OF CONTENTS

INTRODUCTION

Law and society have diverged in their respective perceptions of electronic correspondence. For most people, e-mail is an everyday form of communication, and a proliferation of e-mails has flooded inboxes everywhere. Such volume, coupled with the ability to send, receive, and delete e-mail instantaneously, perpetuates an aura of informality akin to oral conversation. However, in the legal system, and particularly in the context of contract law, e-mails increasingly can and do satisfy formal requirements.

In fact, both state and federal legislatures have legitimized the ability of parties to form contracts electronically. In 2000, the Federal Electronic Signatures in Global and National Commerce Act (E-SIGN)[1] made electronic and paper-and-ink transactions equally enforceable for interstate and foreign contracts.[2] Many states have also adopted the Uniform Electronic Transactions Act (UETA),[3] which

---

[1] 15 U.S.C. §§ 7001 – 7031 (2006).

[2] Holly K. Towle, *Dealing With Contract Formation and Amendment by E-mails*, 743 PRAC. L. INST./PAT. 75, 79-80 (2003) (discussing the impact of e-mails in contract modification in general and in Washington State).

[3] ALA. CODE §§ 8-1A-1 to -20 (LexisNexis Supp. 2002); ALASKA STAT. §§ 09.80.010-.195 (2008); ARIZ. REV. STAT. ANN. §§ 44-7001 to -7051 (2003 & Supp. 2009); ARK. CODE ANN. §§ 25-32-101 to -121 (2002 & Supp. 2001); WEST'S ANN. CAL. CIV. CODE §§ 1633.1-.17 (West Supp. 2010); COLO. REV. STAT. ANN. §§ 24-

establishes that electronic and non-electronic records are equal.[4] Unlike E-SIGN, however, under UETA parties must first agree to contract electronically before this equivalency will be effective.[5] When the parties are silent on the issue, such an agreement will be implied by their use of e-mail to conduct the transaction.[6]

71.3-101 to -121 (West 2008 & Supp. 2009); CONN. GEN. STAT. ANN. §§ 1-266 to -286 (West 2007 & Supp. 2009); DEL. CODE ANN. tit. 6, §§ 12A-101 to -117 (2005 & Supp. 2008); D.C. CODE §§ 28-4901 to -4918 (Supp. 2009); FLA. STAT. ANN. §§ 668.50 (West 2004 & Supp. 2010); HAW. REV. STAT. §§ 489E-1 to -19 (LexisNexis 2009); IDAHO CODE ANN. §§ 28-50-101 to -120 (2005); IND. CODE ANN. §§ 26-2-8-101 to -302 (LexisNexis 2005 & Supp. 2009); IOWA CODE ANN. §§ 554D.101 -.124 (West 2001 & Supp. 2010); KAN. STAT. ANN. §§ 16-1601 to -1620 (2000); KY. REV. STAT. ANN. §§ 369.101-.120 (West 2006 & Supp. 2009); LA. REV. STAT. ANN. §§ 9:2601-2620 (2005 & Supp. 2010); ME. REV. STAT. ANN. tit. 10, §§ 9401-9507 (2009); MD. CODE ANN., COM. LAW §§ 21-101 to -120 (LexisNexis 2005 & Supp. 2009); MINN. STAT. ANN. §§ 325L.01-.19 (West 2000); MASS. ANN. LAWS ch. 110G §§ 1-18 (LexisNexis 2005 & Supp. 2009); MICH. COMP. LAWS ANN. §§ 450.831-.849 (West 2002 & Supp. 2009); MINN. STAT. ANN. §§ 325L.01-.19 (West 2004 & Supp. 2010); MISS. CODE ANN. §§ 75-12-1 to -39 (West 2004 & Supp. 2009); MO. ANN. STAT. §§ 432.200-.295 (West Supp. 2010); MONT. CODE ANN. §§ 30-18-101 to -118 (2008); NEB. REV. STAT. ANN. §§ 86-612 to -643 (LexisNexis 2007); NEV. REV. STAT. §§ 719.010-.350 (2009); N.H. REV. STAT. ANN. §§ 294-E:1-20 (Supp. 2009); N.J. STAT. ANN. §§ 12A:12-1 to -26 (West 2004 & Supp.2009); N.M. STAT. §§ 14-16-1 to -19 (2003 & Supp. 2009); N.C. GEN. STAT. §§ 66-311 to -339 (2009); N.D. CENT. CODE §§ 9-16-01 to -18 (2006 & Supp. 2009); OHIO REV. CODE ANN. §§ 1306.1-.23 (LexisNexis 2009); OKLA. STAT. ANN. tit. 12A, §§ 15-101 to -121 (West 2001 & Supp. 2010); OR. REV. STAT. ANN. §§ 84.001-.061 (West 2003 & Supp. 2009); 73 PA. CONS. STAT. §§ 2260.101-.903 (West 2008 & Supp. 2009); R.I. GEN. LAWS §§ 42-127.1-1 to -20 (2006); S.C. CODE ANN. §§ 26-6-10 to -210 (2007); S.D. CODIFIED LAWS §§ 53-12-1 to -50 (2004 & Supp. 2009); TENN. CODE ANN. §§ 47-10-101 to -123 (2001 & Supp. 2009); TEX. BUS. & COM. CODE ANN. §§ 322.001-.021 (Vernon 2009); UTAH CODE ANN. §§ 46-4-101 to -503 (West 2004 & Supp. 2009); VT. STAT. ANN. tit. 9, §§ 270-290 (2006); VA. CODE ANN. §§ 59.1-479 to -497 (2006 & Supp. 2009); W. VA. CODE §§ 39A-1-1 to -17 (LexisNexis 2004 & Supp. 2009); WIS. STAT. ANN. §§ 137.11-.26 (West 2009); WYO. STAT. ANN. §§ 40-21-101 to -119 (2009).

[4] *See* Robert A. Wittie & Jane K. Winn, *Electronic Records and Signatures under the Federal E-SIGN Legislation and the UETA*, 56. BUS. LAW 293, 294-95 (2000).

[5] Towle, *supra* note 2, at 81.

[6] UNIF. ELEC. TRANSACTIONS ACT § 5, cmt. 4, 7A U.L.A. 211 (West 2002 & Supp. 2009).

Courts seem to follow the lead of these statutes when parties attempt to form or modify a contract by e-mail: the parties' intent governs, regardless of medium. Under common law, parties generally may form or modify contracts by e-mail—even if there is a statutory or contractually imposed writing requirement—so long as all the requisite elements of contract formation are present in the e-mail exchange.[7]

Despite the statutory and common law authority for electronic transactions, most jurisdictions have yet to address the ability of electronic correspondence to effectively modify a contract when the parties' initial transaction is *not* electronic and the parties expressly include a clause that requires all modifications be memorialized in a written and signed document. Such a clause is often called a "no-oral-modification" (NOM) clause because it includes a provision prohibiting oral modification in addition to requiring a signed writing.[8] In

---

[7] Whether or not a statute of frauds has been satisfied requires inquiry into contract formation or modification, which in turn hinges on the parties' intent. The inquiry is therefore fact-specific. Statutes of frauds generally do not require merely writing, but rather a writing that memorializes the contract. Thus many cases find that an e-mail satisfies a statute of frauds writing requirement, but not the statute of frauds. *Compare* Lamle v. Mattel, Inc. 394 F.3d 1355, 1362 (Fed. Cir. 2005) (applying California law to hold that an e-mail constitutes a writing and signature to satisfy California's statute of frauds if the e-mail includes all material terms) *with* Toghiyany v. AmeriGas Propane, Inc. 309 F.3d 1088, 1091 (8th Cir. 2002) (holding that e-mails and a draft agreement did not satisfy Missouri's statute of frauds because they were not signed and did not include a durational term, which is an essential element) *with* Smith v. Int'l Paper Co., 87 F.3d 245, 247 (8th Cir. 1996) (holding an e-mail that does not contain an offer or acceptance does not satisfy the statute of frauds); *and* Illinois Light Co. v. Consolidation Coal Co., 235 F. Supp. 2d 916, 921 (C.D. Ill. 2002) (holding a series of e-mails did not satisfy the statute of frauds because they clearly indicated the parties were negotiating). For a more comprehensive discussion of cases, see John E. Theuman, *Satisfaction of Statute of Frauds by E-Mail*, 110 A.L.R.5th 277 (West 2003 & Supp. 2008) (collecting cases finding e-mails either sufficient or insufficient to satisfy the statute of frauds writing and signature requirements).

[8] *See* BLACK'S LAW DICTIONARY 1159 (9th ed. 2009). For a discussion of NOM clauses in private contracts see RICHARD A. LORD, 10 WILLISTON ON CONTRACTS § 29:42 (4th ed. 2009); E. ALLAN FARNSWORTH, 2 FARNSWORTH ON CONTRACTS § 7.6 (3d ed. 2004). NOM clauses have often been termed private statutes of frauds, and

general, a NOM clause reflects the parties' intent to be bound by modifications only after a final formalized document has been executed, and not by the informal communications that may precede it, such as those that occur during negotiations. Yet even when there is a NOM clause, circumstances may dictate that the contract can be amended, regardless of the medium or the medium's formality.[9] Moreover, even a NOM clause may be modified orally if the parties *intended* to do so.[10]

A few states have implemented statutes requiring that courts disallow such oral modification and give effect to NOM clauses.[11] For example, New York has enacted a law stating that where a contract "contains a provision to the effect that it cannot be changed orally," the contract cannot be modified by an executory agreement unless it is in a signed writing.[12] This statute places New York courts in a position to address whether, in the context of contract modification, an electronic correspondence can constitute a signed writing sufficient to satisfy a NOM clause. The Supreme Court of New York, Appellate Division, decided this very issue in *Stevens v. Publicis, S.A.*, and held that a series of e-mails between the contracting parties satisfied the

---

thus been analogized sections 2-201 and 2-209 of the Uniform Commercial Code (U.C.C.), which provides for NOM clauses in commercial contracts between merchants. For a discussion of a NOM in the U.C.C.'s context see Frank A. Rothermel, Comment, *Role of Course of Performance and Confirmatory Memoranda in Determining the Scope, Operation and Effect of "No Oral Modification" Clauses*, 48 U. PITT. L. REV. 1239 (1987).

[9] *See, e.g.*, Alcon v. Kinton Realty Inc. 2 A.D.2d 454, 456 (N.Y. App. Div. 1956) ("That a written contract may thus be effectively modified, even when it contains a stipulation against oral modification, has long been established. As was said by Judge Cardozo... 'Those who make a contract may unmake it. The clause which forbids a change may be changed like any other.'" (quoting Beatty v. Guggenheim Exploration Co., 122 N.E. 378 (N.Y. 1919) *superseded by statute as stated by* Israel v. Chabra, 906 N.E.2d 374, 377 (N.Y. 2009))).

[10] *See id.*

[11] N.Y. GEN. OBLIG. LAW § 15-301(1) (McKinney 2010). *See also*, TENN. CODE ANN. § 47-50-112(c) (2001); CAL. CIV. CODE § 1698(c) (West 1985); MONT. CODE ANN. §28-2-1602 (2009).

[12] N.Y. GEN. OBLIG. LAW § 15-301(1) (McKinney 2010).

NOM clause in the parties' employment agreement.[13] This Article will first explore the context of the *Stevens* decision by comparing contract modification under New York law to the common law of contract modification. It will then discuss the *Stevens* case and decision. Finally, this Article will explore the implications of *Stevens* for preventing contract modification by e-mail.

I. CONTRACT MODIFICATION IN NEW YORK

Under the common law rule, a contract subject to a statute of frauds writing requirement generally could not be modified by an oral, executory agreement absent consideration[14] unless certain exceptions apply, such as reliance on the modification.[15] However, New York has modified the traditional common law rule by implementing three statutes in chapter 24-A of its General Obligations Law: sections 15-301, 5-1103 and 5-701. Section 5-1103 allows a contract to be modified, even without consideration, as long as there is a signed writing.[16] Thus, this statute is implicated in contracts that contain

---

[13] Stevens v. Publicis, S.A., 50 A.D.3d 253, 255 (N.Y. App. Div. 2008) *leave to appeal dismissed*, 892 N.E.2d 399 (N.Y. 2008).

[14] *See* RICHARD A. LORD, 3 WILLISTON ON CONTRACTS § 7:8 (4th ed. 2009) ("It is therefore generally true that promises, in order to be enforceable, need consideration."). *See also* RESTATEMENT (SECOND) OF CONTRACTS § 79 (1981) (setting forth the general rule that "If the requirement of consideration is met, there is no additional requirement of (a) a gain, advantage, or benefit to the promisor or a loss, disadvantage, or detriment to the promisee; or (b) equivalence in the values exchanged; or (c) 'mutuality of obligation.'")

[15] RESTATEMENT (SECOND) OF CONTRACTS § 89 (1981) (allowing for three instances when modification of a contract that has not been fully performed becomes binding: (1) if it would be "fair and equitable" in light of changed circumstances; (2) if authorized by statute; and (3) if justice would so require because of a "material change of position in reliance."). *See also* RESTATEMENT (SECOND) OF CONTRACTS § 89 cmt. a (1981); RESTATEMENT (SECOND) OF CONTRACTS § 149(2) (1981) ("The Statute of Frauds may prevent enforcement in the absence of reliance."); RESTATEMENT (SECOND) OF CONTRACTS § 150 (1981) (stating that even if the statute of frauds is applicable, the contract may be modified orally if there has been "a material change of position in reliance" on the oral modification).

[16] N.Y. GEN. OBLIG. LAW § 5-1103 (McKinney 2010).

NOM clauses insofar as they require a signed writing to effect modification. As mentioned, section 15-301 mandates court enforcement of NOM clauses.[17] Since section 15-301 reinforces a NOM's signed writing requirement by requiring that courts give effect to NOM clauses,[18] sections 5-1103 and 15-301, taken together, ensure that a signed writing may modify a contract with a NOM clause regardless of whether consideration is provided.

New York's general statute of frauds, codified in section 5-701,[19] also plays a role in the enforcement of NOM clauses in New York. The purpose of the signature requirement in section 15-301 is to authenticate assent to proposed modifications.[20] In a similar vein, section 5-701, as a statute of frauds, requires that certain contracts be memorialized in a signed writing[21] and shares this authentication purpose, albeit at contract formation.[22] Courts in New York have drawn on precedent construing section 5-701 by analogy when interpreting the signature requirement in section 15-301.[23] Thus,

---

[17] N.Y. GEN. OBLIG. LAW § 15-301 (McKinney 2010).

[18] *Id.*

[19] N.Y. GEN. OBLIG. LAW § 5-701 (McKinney 2010).

[20] *See* Israel v. Chabra, 537 F.3d 86, 100 (2nd Cir. 2008), *certified question answered*, 906 N.E.2d 374 (N.Y. 2009), *vacated to conform to answer to certified question*, 601 F.3d 57 (2nd Cir. 2010) (noting the purpose of section 15-301(1) was "to assure the authenticity of an amendatory agreement; thus, the statute requires the dignity of a formal writing to insure the validity and genuineness of a contractual modification." (citing DFI Commc'ns, Inc. v. Greenberg, 363 N.E.2d 312, 315 (N.Y. 1977))).

[21] *Id.*

[22] *See* Parma Tile Mosaic & Marble Co., Inc. v. Estate of Short, 663 N.E.2d 633, 634 (N.Y. 1996) (holding that a name automatically printed on a facsimile does not satisfy the statute of frauds requirement because doing so does not evince a present intent to authenticate the document's contents).

[23] *See, e.g.*, DFI Commc'ns, Inc. v. Greenberg, 363 N.E.2d 312, 315 (N.Y. 1977) (distinguishing the statutes, but also recognizing their similar purpose in holding that signed meeting minutes may be sufficient to satisfy sections 15-301 and 5-701). *See also* Rochester Cmty. Individual Practice Ass'n v. Finger Lakes Health Ins. Co., 281 A.D.2d 977, 978 (N.Y. App. Div. 2001) (drawing on Parma Tile Mosaic & Marble Co., Inc. v. Estate of Short, 663 N.E.2d 633, 634 (N.Y. 1996) to interpret section 5-701 to construe section 15-301).

section 15-301 coupled with the jurisprudence interpreting New York's statute of frauds effectively prevents modification without a signed writing. [24]

There are, however, ways around a NOM's writing requirement, even when such statutes mandate enforcement. Again, under common law, a contract without a NOM clause can be modified orally without consideration and without a signed writing if there is reliance.[25] If the contract has a NOM clause, the parties must have both relied on the contract modification and waived the writing requirement. Generally, oral attempts to modify a contract may waive a statutorily imposed writing requirement such as the statute of frauds.[26] However, even if the writing requirement is waived by oral attempts to modify, the contract will not be modified unless there is also reliance.[27] Indeed, in construing 15-301, New York courts have added that, to waive the NOM clause, an attempt to orally modify must be accompanied by reliance.[28]

Often, attempts at contract modification are accompanied by reliance. In these situations, the issue of whether an e-mail exchange is a writing that satisfies a NOM clause is irrelevant because the writing requirement has been waived.[29] In fact, courts in New York[30] and

---

[24] N.Y. GEN. OBLIG. LAW § 5-701 (McKinney 2010).

[25] *See supra* note 15.

[26] RICHARD A. LORD, 10 WILLISTON ON CONTRACTS § 29:42 (4th ed. 2009) (discussing whether an attempt to modify alone is sufficient, or whether reliance is also necessary). *Cf.* RICHARD A. LORD, 3 WILLISTON ON CONTRACTS § 7:38 (4th ed. 2009) (discussing contract modification in the sale-of-goods context under the U.C.C.).

[27] RICHARD A. LORD, 10 WILLISTON ON CONTRACTS § 29:42 (4th ed. 2009); RESTATEMENT (SECOND) OF CONTRACTS § 84 (1981).

[28] *See, e.g.*, The Savage is Loose Co. v. United Artists Theatre Circuit, Inc., 413 F. Supp. 555, 559 (S.D.N.Y. 1976) (requiring reliance based on oral modification in order to effectively waive a NOM clause and modify a contract).

[29] RICHARD A. LORD, 10 WILLISTON ON CONTRACTS § 29:42 (4th ed. 2009).

[30] *See, e.g.*, The Savage is Loose Co. v. United Artists Theatre Circuit, Inc., 413 F. Supp. 555, 559 (S.D.N.Y. 1976) (requiring reliance on oral statements to modify a contract, although the oral statements themselves waive the writing requirement); Canizaro v. Mobile Commc'ns Corp. of America, 655 So. 2d 25, 30 (Miss. 1995)

elsewhere allow modification—regardless of the medium—when an attempt to modify is accompanied by reliance.[31] In New York, however, an attempt to modify alone, absent reliance, does not necessarily waive the NOM clause. To overcome a NOM clause and effectively modify the contract, an e-mail exchange must be deemed a writing with sufficient formality to satisfy section 15-301 and therefore the statute of frauds.

II. *STEVENS V. PUBLICIS*: E-MAIL CAN SATISFY A NOM CLAUSE

In *Stevens*, the New York Supreme Court, Appellate Division, in a succinct slip opinion, held that a series of e-mails between contracting parties satisfied the requirements of an enforceable NOM clause, even without waiver or reliance.[32] The result dispels the aura of informality surrounding e-mails and presumes they are signed writings. The *Stevens* decision suggests that to avoid modification by e-mail, contracting parties should include "no e-mail modification" (NEM) clauses in their contracts.[33]

The events that precipitated *Stevens v. Publicis, S.A.* began when Publicis, S.A. (Publicis) purchased Arthur Stevens' public relations firm, Lobsenz-Stevens.[34] The parties entered into both an employment contract and a stock purchase agreement (SPA).[35] Under the employment contract, Stevens was to remain as CEO for three years.[36] The

(noting that oral modification was effective, and waived a NOM clause when there was reliance, and analogizing the situation to statutory NOM clauses as exemplified by section 2-209 of the U.C.C.); Varnell v. Henry M. Milgrom, Inc., 337 S.E.2d 616, 619 (N.C. Ct. App. 1985) (requiring both oral statements and conduct indicating reliance on those statements to modify a contract subject to the U.C.C.'s statute of frauds writing requirement).

[31] RICHARD A. LORD, 10 WILLISTON ON CONTRACTS § 29:42 (4th ed. 2009).

[32] *Stevens*, 50 A.D.3d at 256.

[33] *See* Towle, *supra* note 2, at 78-79 (suggesting that parties wishing to avoid contract modification by e-mail may be well advised to include a notice to that effect in the contract and possibly in their e-mails).

[34] *Stevens*, 50 A.D.3d at 254.

[35] *Id.*

[36] *Id.*

SPA correspondingly provided Stevens with performance incentives via an earn-out provision that increased the purchase price of the stocks that Publicis would buy from Stevens based upon the firm's success over those three years.[37] The employment contract had a NOM clause expressly stating that any amendments had to be memorialized in a written and signed document.[38]

After six months, the company's business stalled and Stevens was relieved of his position as CEO.[39] Pending his removal, Stevens exchanged a series of e-mails with an executive at Publicis.[40] The e-mails proposed that Stevens continue to work at the firm, but detailed a new job description, which Stevens clarified and then accepted by e-mail.[41] Stevens later sued Publicis for breaching the employment contract by removing him from his position as CEO before the three-year earn-out period had ended.[42]

Stevens asserted that the e-mail exchange did not effectively modify his employment contract because the e-mails neither explicitly referred to the contract, nor declared that they would constitute a modification to the employment contract.[43] He argued that absent unequivocal expressions of both parties' intent to contract by e-mail, the exchange could not overcome the contractual requirement that modifications be formalized in a signed writing.[44] The court disagreed and, without clarifying its rationale in detail, stated that an e-mail constitutes a signed writing sufficient to satisfy both the statute of frauds and the employment contract's clause requiring a signed writing for modification.[45]

---

[37] *Id.*

[38] Brief of Defendant-Respondent at 30, Stevens v. Publicis, S.A., 50 A.D.3d 253 (N.Y. Sup. Ct. 2008) (No. 602716/03).

[39] *Id.*

[40] *Stevens*, 50 A.D.3d at 254-55.

[41] *Id.*

[42] *Id.* at 254.

[43] Brief of Plaintiff-Appellant at 33, Stevens v. Publicis, S.A., 50 A.D.3d 253 (N.Y. Sup. Ct. 2008) (No. 602716/03).

[44] *Id.*

[45] *Stevens*, 50 A.D.3d at 255-56.

The court relied on the New York case *Rosenfeld v. Zerneck*,[46] which interprets the statute of frauds requirements under section 5-701.[47] In *Rosenfeld*, the New York Supreme Court held that the statute of frauds' "signed writing" requirement may be satisfied by e-mail.[48] In *Rosenfeld*, the defendant used e-mail to accept an oral offer to sell real property and indicate that his attorney would "prepare a contract of sale."[49] Although this language suggests intent to contract, it also implies a subjective belief that the parties would not be bound until a formal written contract had been drafted and signed. Nonetheless, the court in *Rosenfeld* stated that if the e-mail exchange had included all vital contract terms, it would have enforced the e-mail contract.[50] The *Stevens* Court used the *Rosenfeld* decision to support the proposition that an e-mail is a writing sufficient to satisfy the statute of frauds.[51] Therefore, an e-mail may also satisfy the writing requirement of the NOM as enforced by section 15-301.

The "signature" requirement of the NOM clause was deemed satisfied in *Stevens* by the parties' typed names at the end of each e-mail.[52] The court did not cite any authority for this assertion, although it followed directly after a discussion of *Rosenfeld*, where the court did find that a typed signature on an e-mail satisfied the signature requirement of the statute of frauds.[53] The *Rosenfeld* Court

---

[46] 4 Misc. 3d 193 (N.Y. Sup. Ct. 2004).

[47] *Stevens*, 50 A.D.3d at 255-56 (citing *Rosenfeld*, 4 Misc.3d at 195). *See also* Bazak Int'l Corp. Tarrant Apparel Group, 378 F. Supp.2d 377, 386 (S.D.N.Y. 2005) (finding that an e-mail exchange satisfies the statute of frauds for sections 2-201 and 2-209 of New York's U.C.C.). *But see* Vista Developers Corp. v. VFP Realty, LLC, 17 Misc. 3d 914, 920-21 (N.Y. Sup. Ct. 2007) (holding that section 5-703 of New York's General Obligations Law governs contracts for the sale of real property and under this provision an e-mail exchange is not sufficient to satisfy the statute of frauds' writing requirement).

[48] *Rosenfeld*, 4 Misc. 3d at 194.

[49] *Id.*

[50] *Id.* at 196.

[51] *Stevens*, 50 A.D.3d at 255-56.

[52] *Id.*

[53] *Rosenfeld*, 4 Misc. 3d at 195 (distinguishing Parma Tile Mosaic & Marble Co. v. Estate of Short, 663 N.E.2d 633 (N.Y. Ct. App. 1996), where a fax transmission

decided that, since the name on the e-mail was intentionally typed, it clearly indicated intent to authenticate.[54] The *Stevens* Court again seemed to extend the *Rosenfeld* holding on the statute of frauds to NOM clauses, and infer that the intent to authenticate for statute of fraud purposes was the same intent required to satisfy a NOM clause.[55]

The *Stevens* Court did not explicitly extend the holding to contracts containing NOM clauses, although that is the effect of the decision.[56] Moreover, the *Stevens* decision could be broader in that an e-mail can satisfy both statutorily imposed formal writing requirements and those imposed by contractual clauses. Further, the *Stevens* decision indicates that NOM clauses may not bar unintended contracting by e-mail. On the other hand, the effect of the holding may be limited to New York law. Still, the decision reflects a trend in favor of electronic contracting.[57] Contract drafters must use particular care to avoid contract modification by e-mail—if that is their intent.

III. HOW TO PREVENT MODIFICATION BY E-MAIL

The most obvious lesson to be drawn from the *Stevens* decision is that a clause stating that all modifications to a contract must be in writing—or even a "signed" writing—does not necessarily preclude amendment via e-mail. A NOM clause may not be sufficient to prevent contract modification by e-mail unless the parties expressly state their intention to not be bound by e-mail amendments or expressly define the manner of contract modification.

---

that automatically put the sender's name on each page did not meet the signature requirement for the statute of frauds).

[54] *Id.* at 195-96.

[55] *Stevens*, 50 A.D.3d at 256.

[56] *Stevens*, 50 A.D.3d at 255-56.

[57] *See* Anita Ramasastry, *A New York Appellate Court Holds That an Email Message Can Amend an Employment Contract: Why the Decision Was Correct, and What it Means for Employees*, FINDLAW, May 29, 2008, http://writ.lp.findlaw.com/ramasastry/20080529.html. For a discussion of the trend toward enforcing electronic contract formation and modification see Wittie & Winn, *supra* note 4, at 294-95.

A. *Explicitly State Intent Not to be Bound by E-Mail Amendments*

Courts in New York have enforced NOM clauses pursuant to section 15-301.[58] Moreover, courts are likely to uphold NOM clauses if viewed as expressions of the parties' intent not to contract orally.[59] Therefore, *Stevens* illustrates the wisdom of including an explicit expression of intent *not* to contract by e-mail: in essence, a "no e-mail modification" (NEM) clause.[60] Besides using a NEM clause, parties may use several other drafting techniques to prevent e-mail modification. For instance, the contract may also enumerate the procedures necessary to effectively amend it, and specifically exclude e-mails as an acceptable means of satisfying a NOM clause. The contract may also include a statement defining a signed writing as a "handwritten (not electronic) signature."

Paradoxically, in the absence of a NEM clause, a court may actually be inclined to favor modification by e-mail. Courts prefer accurate manifestations of parties' intent over the formalities of written contracts.[61] Therefore, courts often favor handwritten or typed documents over pre-printed ones, since the former are more likely to reflect true intent, and less likely to contain boilerplate language.[62] As a

---

[58] *See, e.g.*, Lewis v. Rahman, 147 F. Supp.2d 225, 235 (S.D.N.Y. 2001) (citing section 15-301 to assert that "[w]here, as here, the contract to be modified provides that all modifications must be in writing, a purported oral modification violates the Statute of Frauds."). *But see* Rose v. Spa Realty Assocs., 366 N.E.2d 1279, 1282-83 (N.Y. 1977) (noting that when the only proof of modification is the oral exchange itself, the NOM will be enforced, but if the oral modification has been acted upon—in other words, if there is reliance—then the oral modification may be effective).

[59] *See, e.g.*, CrossLand Fed. Sav. Bank by F.D.I.C. v. A. Suna & Co., Inc., 935 F. Supp. 184, 197 (E.D.N.Y. 1996) (stating that "[w]here the parties have demonstrated an intent not to be bound until they have executed a formal contract, they cannot be bound until the writing is complete.").

[60] *See also* Towle, *supra* note 2, at 91 (noting that "no one is forced to deal electronically if they do not want to, at least as to general contractual matters.").

[61] *See* ROBERT A. FELDMAN & RAYMOND T. NIMMER, DRAFTING EFFECTIVE CONTRACTS: A PRACTITIONER'S GUIDE, § 1.03A[B] (2d ed. 1999 & Supp. 2008).

[62] *See also, e.g.*, Patel v. United Inns Inc., 887 N.E.2d 139, 148-49 (Ind. Ct. App. 2008), *transfer dismissed*, 887 N.E.2d 139 (Ind. 2009) (stating that "[w]hen construing

result, e-mails may potentially be given additional weight *because* they are perceived as less formal.[63]

B. Make the Manner of Modification Explicit

If including NEM clauses in contracts and appending disclaimers to e-mails becomes routine, however, courts might eventually consider their language boilerplate as well.[64] If this occurs, then courts are likely to treat NEM clauses and other disclaimers as they do NOM clauses: overlook them when the e-mails indicate intent to contract or when other special circumstances, such as reliance, are present. Such a result may be avoided with explicit statements of what will or will not effectively modify the contract, both at the outset of contract formation and during negotiations for a modification itself. At contract formation, this explicit statement could simply be a written statement in the contract describing the manner or procedures for modification. During contract amendment negotiations, the issue could be addressed in multiple ways. For instance, a disclaimer stating

---

a contract where there is apparent conflict, handwriting prevails over typewriting." In footnote 3, the court also notes that handwritten terms are favored because "there is a presumption that the handwritten terms were more actively negotiated between the parties, and, therefore, that those terms best reflect the parties' intent." The court cites State v. Scott Constr. Co., 174 N.E. 429, 431 (Ind.Ct. App. 1931) and Sprague Elec. Co. v. Bd. Comm'rs Hennepin County, 86 N.W. 332, 333 (Minn. 1901) to support this assertion).

[63] *See, e.g.*, Otto Interiors, Inc. v. Nestor, 196 Misc.2d 48, 50 (N.Y. Civ. Ct. 2003) (finding that a typewritten provision was preferable to a printed form because it was a truer reflection of the parties intentions) (citing Lanni v. Smith, 89 A.D.2d 782, 783 (N.Y. App. Div. 1982)); *see also*, Ganisin v. Noeth, 163 A.D.2d 828, 829 (N.Y. App. Div. 1990) ("By setting forth the method by which the contract may be amended, to wit, by a writing, it implies the preclusion of other less formal methods of amendment.")

[64] *Chicago Inv Corp. v. Dolins*, 481 N.E.2d 712, 715 (Ill. 1985) (characterizing a provision in letters of intent exchanged by the parties, which provided that a formal document would be executed, as "mere recitation"— particularly when there was evidence that the parties intended to be bound by the terms of those letters. However, the court also noted that "parties may specifically provide that negotiations are not binding until a formal agreement is in fact executed.").

the sender's intent not to modify the contract could be included in the body of every e-mail. Since modifications are themselves specifically negotiated, such statements included within them are unlikely to be perceived as boilerplate.

CONCLUSION

Stevens v. Publicis, S.A. raises electronic correspondence to the level of a formal, signed writing in New York. The case signals that e-mails may be treated as written, signed documents—even when the parties' do not express intent to treat them as such. In addition, statutory legitimization of electronic contracting, common law precedents allowing contract formation and modification by e-mail , and common law precedents upholding the sufficiency of an e-mail as a signed writing for statute of frauds purposes all suggest that *Stevens* is part of a trend towards making e-mails the formal equivalent to paper and ink. To avoid being bound by e-mailed conversations, it is important not only to exercise caution in e-mailing, but also in drafting and negotiating contracts at the outset to expressly deal with e-mail as a possible method of modification.

PRACTICE POINTERS

- Standard "no-oral-modification" (NOM) clauses may be insufficient to prevent contract modification via e-mail.
- Parties should explicitly state in their contract that amendments cannot be made by electronic correspondence or that a signed writing requires a handwritten—not electronic—signature.
- Where parties are discussing possible amendments to an existing contract via e-mail, disclaimers should be included in the text of such e-mails indicating that the correspondence does not satisfy the NOM clause or constitute an amendment to the contract.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 6, ISSUE 1 SUMMER 2010

TRUSTING THE MACHINES: NEW YORK STATE BAR ETHICS OPINION ALLOWS ATTORNEYS TO USE GMAIL

Kevin Raudebaugh[*]

CITE AS: 6 WASH. J.L. TECH. & ARTS 83 (2010),
https://digital.lib.washington.edu/dspace-law/handle/1773.1/452

ABSTRACT

Information technology is evolving at an unprecedented rate; new forms of communication appear so often that it is difficult to keep track of them all. This presents a difficult problem for attorneys, who must carefully consider whether using new technology to communicate with clients is consistent with the duty of confidentiality. Google's Gmail scans the content of e-mails to generate targeted advertising, a controversial practice that raises questions about whether its users have a reasonable expectation of privacy. The New York Bar responded to this issue in Opinion 820, which states that using an e-mail provider that scans the e-mail content to display relevant advertising does not violate a lawyer's duty of client confidentiality. This article explains the controversial nature of Gmail, the evolution of e-mail in ethics opinions, and Opinion 820's content and implications.

TABLE OF CONTENTS

---

[*] Kevin Raudebaugh, University of Washington School of Law, Class of 2010. Many thanks to Professors Anita Ramasastry and Andrew Perlman for their expert guidance on this subject.

INTRODUCTION

The use of free e-mail providers has become virtually ubiquitous in electronic communication. But while the majority of e-mail users do not directly pay for Internet-based services, these services do have the potential to generate income. Many e-mail providers recoup some of their costs by placing advertisements inside the e-mail viewing window, or even within the e-mail itself.

Some of the more successful e-mail providers have found ways to target ads to the characteristics of a particular user, which makes the ads more valuable to advertisers than mere random placement. Most providers gather targeting information by monitoring user activities within the providers' domains,[1] such as which ads users click on, which areas of the providers' domain they visit, or even which other Web sites they visit.[2] But one e-mail provider, Google's Gmail, has attracted controversy by gathering information for targeted advertising with software that scans the actual content of e-mails.

Attorneys, through their duty of confidentiality, must ensure that their communications remain private and confidential.[3] Due to the popularity of Gmail, attorneys will likely be corresponding with some clients who use Gmail addresses. Although a number of states have issued ethics opinions on the impact of the duty of confidentiality on e-mail,[4] the New York State Bar is the first to consider Gmail's practice

---

[1] In this context, the term "domain" refers to a lower level domain of the Domain Name System (DNS). The three-letter extension such as ".com" or ".net" is a top-level domain, and lower level domains are any word that appears to the left of the extension, such as "Google" or "Yahoo."

[2] For a summary of how targeted online advertisements are generally gathered and delivered, see Testimony of Edward W. Felten, *Behavioral Advertising: Industry Practices and Consumers' Expectations: Hearing Before the H. Comm. on Energy and Commerce the Subcomm. On Commc'ns, Tech. and the Internet, and the Subcomm. On Commerce, Trade and Consumer Prot.*, 111th Cong. (2009) (June 18, 2009), *available at* http://www.cs.princeton.edu/~felten/testimony_18june2009.pdf. In addition to email providers, many web portals and social networking services collect user data for targeted advertisements.

[3] MODEL RULES OF PROF'L CONDUCT R. 1.6 (2009).

[4] So far, at least 22 states have issued ethics opinions regarding the use of e-mail

of actually scanning the text of e-mail messages. The New York opinion concludes that using e-mail services that scan content to generate targeted advertising does not breach the duty of confidentiality so long as the information is not reviewed by humans.[5]

This Article analyzes the New York Bar opinion. It first describes how Gmail conducts targeted advertising. It then reviews the history of bar opinions related to new communications technologies and explains how they have evolved. Next, it examines the nature of the controversy over Gmail. Last, it explains how the New York Bar opinion resolved those issues and discusses key implications of the opinion.

I. GMAIL AND TARGETED ADVERTISING

The New York State Bar Opinion directly implicates Gmail, a popular Web-based e-mail service run by Google. Gmail is a free, Web-based e-mail service with a very large storage capacity.[6] Gmail is currently the third most popular e-mail provider, with over 113 million users worldwide.[7] With such a large user base, it is likely that attorneys

---

and the duty of confidentiality. Alaska Bar Ass'n Ethics Comm. Op. 98-2 (1998); St. Bar Ariz. Comm. Rules of Prof'l Conduct Adv. Op. 97-04 (1997); Conn. Bar Ass'n Ethics Op. 99-52 (1999); D.C. Bar Op. 281 (1998); Fla. St. Bar Ass'n Ethics Op. 00-4 (2000); Ill. St. Bar Ass'n Adv. Op. 96-10 (1997); Iowa Sup. Ct. Bd. Prof'l Ethics Conduct Op. 97-01 (1997); Ky. Bar Ass'n Ethics Op. E-403 (1997); Me. Prof. Ethics Comm. Bd. of Overseers of the Bar Ethics Op. 195 (2008); Mass. Bar Assoc. Comm. Prof'l Ethics Adv. Op. 00-1 (1998); Md. Law. Prof. Resp. Bd. Op. No. 19 (1992); Minn. Law. Prof. Resp. Bd. Ethics Op. 19 (1999); Mo. St. Bar Legal Ethics Counsel Adv. Op. 970230 (1997); N.Y. St. Bar Ass'n Comm. Prof'l Ethics Op. 820 (2008) N.C. St. Bar Ethics Op. RPC 215 (1995); St. Bar Ass'n of N.D. Ethics Comm. Op. No. 97-09 (1997); Ohio Bd. Com. Griev. Disp. Adv. Op. 99-2 (1999); Pa. Bar Ass'n Comm. Ethics Prof. Resp. Op. 97-130 (1997); S.C. Bar Ethics Adv. Comm. Op. 97-08 (1997); Sup. Ct. Tenn. Bd. of Prof'l Resp. Adv. Op. 98-A-650(a) (1998); Utah St. Bar. Ethics Op. 00-01 (2000); Vt. Adv. Ethics Op. 97-5 (1997). Hereinafter, these opinions will be referred to as Advisory Opinions (Adv. Op.) or Ethics Opinions (Ethics Op.).

[5] NY Ethics Op. 820 (2008).

[6] Gmail launched with two gigabytes of storage capacity per user. Currently, the storage capacity is over seven gigabytes, and it is still growing.

[7] Chua Hian Hou, *Gmail Users Locked Out*, THE STRAITS TIMES, Feb. 25, 2009, http://www.straitstimes.com/Breaking%2BNews/Singapore/Story/STIStory_342

will be expected to send e-mail correspondence to Gmail accounts.

Gmail generates revenue by displaying advertisements next to the content of the messages. In order to tailor these advertisements to the Gmail user, Google's software scans the content of an open e-mail for relevant text and then displays advertisements related to that text.[8] For instance, if a Gmail user opens an e-mail about an upcoming trip to Chicago, the web interface might display ads for hotels and restaurants in Chicago. The advertisements are entirely text-based, which minimizes both the effect on the user and bandwidth usage.

Gmail's process of scanning e-mail content and matching it to advertisements is entirely automated.[9] Humans are not directly involved with the process, and the information gleaned from the e-mails is not disclosed to any third parties, including the advertisers.[10] The ad content is dynamically generated when an e-mail is opened, meaning that ad content is not attached to particular accounts.[11] Although Google's patent on the technology covers the ability to create logs of user profiles, which can include keywords and potentially sensitive data,[12] Google's Vice President of Engineering stated that Gmail does not use this feature.[13]

Automated scanning of e-mail content is not unique to Gmail. Virtually every e-mail service conducts similar automated scanning for many purposes, including "spam filtering, virus detection, search, spellchecking, forwarding, auto-responding, flagging urgent messages, converting incoming e-mail into cell phone text messages, automatic saving and sorting into folders, converting text URLs to clickable links, and reading messages to the blind."[14] The primary difference between

---

818.html. The other top e-mail providers are Hotmail (283 million) and Yahoo (274 million).

[8] Google, About Gmail, Jan. 2007, http://mail.google.com/mail/help/about_privacy.html#scanning_email (on file with the author).

[9] *Id.*

[10] Google, About Gmail, Jan. 2007, http://mail.google.com/mail/help/about_privacy.html#targeted_ads (on file with the author).

[11] *Id.*

[12] Electronic Privacy Information Center, Gmail Privacy Page, Aug. 8, 2004, http://epic.org/privacy/gmail/faq.html#23.

[13] Kim Zetter, *Free Email With a Steep Price?*, WIRED, April 1, 2004, http://www.wired.com/techbiz/media/news/2004/04/62917.

[14] Google, About Gmail, Jan. 2007, http://mail.google.com/mail/help/about

Gmail's targeted advertising technology and these other uses is that Gmail's scanning generates income from third-party advertisers, while the other uses are typically billed as services for the user.

II. ELECTRONIC COMMUNICATIONS AND CONFIDENTIALITY

The legal ethics community has been cautious about the ability of lawyers to maintain the confidentiality of communications in newly introduced electronic media. For example, when cell phones were first introduced, federal courts did not find a reasonable expectation of privacy in their use, partially because no law directly prohibited interception of their signals.[15] Then in 1986, Congress passed the Electronic Communications Privacy Act (ECPA), which made it illegal to intentionally intercept electronic transmissions.[16] Following the protection of the ECPA and advances in cell phone technology from analog to digital transmissions, state bars found their use consistent with an attorney's duty of confidentiality.[17]

The American Bar Association (ABA) first considered the issue of e-mail confidentiality in 1986. The ABA concluded that before communicating client confidences over an electronic network, attorneys needed to obtain bar approval or make an informed opinion regarding the system's reliability in maintaining confidentiality.[18] Similarly, the initial state bar ethics opinions held that unfettered use of e-mail was not consistent with the duty of confidentiality. A 1995 ethics opinion from South Carolina required express waivers from the

---

_privacy.html#targeted_ads (on file with the author).

[15] *See* Tyler v. Berodt, 877 F.2d 705 (8th Cir. 1989) (finding that cell phone communications are not protected by the Wiretap Act, and noting that the events in question occurred before the ECPA was passed).

[16] 18 U.S.C. § 2511(1) (2008). The ECPA was written to apply to cell phone communication, but it was amended in 1994 to apply to cordless telephone communication and e-mail. Mitchel L. Winick, Brian Burris & Y. Danae Bush, *Playing I Spy with Client Confidences: Confidentiality, Privilege and Electronic Communications*, 31 TEX. TECH L. REV. 1225, 1242-1248 (2000).

[17] Mark W. Pearlstein & Jonathan D. Twombly, *Cell Phones, Email, and Confidential Communications: Protecting Your Client's Confidences*, 46 B. B.J. 20, 21 (2002).

[18] Winick, et al., *supra* note 16, at 1249.

clients unless confidentiality was certain,[19] and a 1996 ethics opinion from Iowa required encryption of sensitive materials.[20] After the Iowa opinion, no other state opinions required encryption except in unusual circumstances.[21] Both the Iowa and South Carolina opinions were later amended to remove the encryption requirements.[22]

In 1999, after extensively reviewing the issue, the ABA issued a formal opinion on e-mail confidentiality.[23] The opinion analyzes risks associated with all modes of e-mail transmission, considers the security of alternative means of communication, and notes the statutory protections for illicitly intercepting e-mail.[24] It concludes "lawyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure."[25] The opinion states that while some state bars have required express consent from clients, "more recent opinions reflecting lawyers' greater understanding of the technology involved approve the use of unencrypted Internet e-mail without express client consent."[26] The opinion also recommends, but does not require, that attorneys use encryption in sensitive e-mail communications.[27]

---

[19] S.C. Bar Ethics Adv. Comm. Op. 94-27 (1995).

[20] Iowa Sup. Ct. Bd. Prof'l Ethics Conduct Op. 95-30 (1996).

[21] Winick, et al., *supra* note 16, at 1253. Some opinions, such as the opinion from Connecticut, describe these as being circumstances "which would place a lawyer on notice that there is a greater than ordinary risk of interception or unauthorized disclosure (such as an e-mail "mailbox" which is accessible to persons other than the intended recipient) . . ." Conn. Ethics Op. 99-52 (1999).

[22] *See* Iowa Ethics Op. 96-01 (1996); S.C. Adv. Op. 97-08 (1997). The amended Iowa opinion now provides that "with sensitive material to be transmitted on e-mail, counsel must have written acknowledgment by client of the risk of violation of DR 4-101 which acknowledgment includes consent for communication thereof . . . or it must be encrypted or protected by password/fire-wall or other generally accepted equivalent security system."

[23] ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999).

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

III. PRIVACY CONCERNS SURROUNDING GMAIL

When Google introduced its Gmail service in March 2004, it was met with widespread distrust from privacy advocates. Within one month, 31 privacy and civil liberties organizations published an open letter to Google decrying the practice of scanning e-mails for targeted advertisements.[28] The letter argues that scanning e-mails "violates the implicit trust of an e-mail service provider," that Google's policies lacked clarity, and that the scanning set a precedent for reduced expectations for privacy.[29] Regarding the actual privacy of the content, the letter states that "a computer system, with its greater storage, memory, and associative ability than a human's, could be just as invasive as a human listening to the communications, if not more so."[30] The controversy was so great that it even provoked legislation in California.[31]

Numerous technology and business advocates—and even some prominent privacy advocates—criticized the outcry against Gmail.[32] Those organizations maintained that the harm envisioned by Gmail's opposition was largely hypothetical, Gmail was operating within the bounds of the law, and there was no real threat that private information would be divulged to humans, which was the central

---

[28] Privacyrights.org, Thirty-One Privacy and Civil Liberties Organizations Urge Google to Suspend Gmail, April 6, 2004, http://www.privacyrights.org/ar/GmailLetter.htm. The letter acknowledges that the scanning technology is essentially as invasive as scanning for spam or viruses, but insists that displaying ads "is fundamentally different than removing harmful viruses and unwanted spam."

[29] *Id.*

[30] *Id.*

[31] In the same month that the open letter was issued, April of 2004, California State Senator Liz Figueroa introduced SB1822, Ban on Secretly Scrutinizing E-Mail Messages for Targeted Advertising. Grant Yang, *Stop the Abuse of Gmail*, 2005 DUKE L. & TECH. REV. 14, 23 (2005). The bill would allow e-mail providers to derive information from the content of their communications, but would prohibit using it for the provider's marketing purposes. Thus, scanning for antivirus or spam removal would be legal, but Gmail's scanning for targeted advertising would not be. The legislation was ultimately abandoned.

[32] Brad Templeton, Privacy Subtleties of Gmail, http://www.templetons.com/brad/gmail.html (last visited May 2, 2010). Brad Templeton is the chairman of the Electronic Frontier Foundation.

concern of both privacy groups and attorney confidentiality.[33] Nevertheless, the controversy has followed Gmail and may have been the impetus for the New York State Bar to consider the implications on attorney-client confidentiality.

IV. THE NEW YORK STATE BAR OPINION AND ITS IMPLICATIONS

Opinion 820 starts by pointing out that a previous New York State Bar Opinion found a reasonable expectation of privacy in the use of unencrypted e-mail.[34] The prior opinion states that a lawyer may not transmit client confidences by e-mail where there is a heightened risk of interception, and that a lawyer "who uses internet e-mail must also stay abreast of this evolving technology to assess any changes in the likelihood of interception."[35] Hence, Opinion 820 asks whether Gmail's scanning for targeted advertising presents a heightened risk as a new technology. Although Gmail is never specifically named, the opinion refers to "the particular e-mail provider's published privacy policies," implying a focus on Gmail.[36] The opinion observes that according to those privacy policies, no humans will be exposed to the e-mail content, and therefore concludes that the risks to confidentiality

---

[33] *See* Nicole A. Wong, *Google's Gmail and Privacy Policy*, 797 PRAC. L. INST./ PAT. 263 (2004). The article consists of exerts from prominent publications and organizations complied by an attorney for Google that support Gmail's privacy policy and technology.

[34] N.Y. St. Bar Ass'n Comm. Prof'l Ethics Op. 709 (1998).

[35] *Id.* A number of other state e-mail confidentiality opinions have similar caveats to their permission that could be grounds for later exceptions under particular circumstances. *See, e.g.*, DC Ethics Op. 281 (1998) ("absent special factors"); Mass. Adv. Op. 00-1 (1998) (use of e-mail "does not, *in most instances*, constitute a violation…") (emphasis added); Md. Ethics Op. 19 (1999) ("precautions taken by a lawyer depend on the circumstances"); Me. Ethics Op. 195 (2008) ("reasonable judgment may require additional safeguards depending on the circumstances); Tenn. Adv. Op. 98-A-650(a) ("unless unusual circum-stances require enhanced security measures"); Utah Ethics Op. 00-01 (2000) (when "the lawyer has reason to believe that the risk of interception is higher, he may want to use a means of communication with higher security"). New York's opinion, however, appears to be the only one that requires lawyers to stay abreast of evolving e-mail technology to reassess the issue, and hence they may be the only state that issues an opinion on Gmail.

[36] N.Y. Ethics Op. 820 (2008).

through Gmail are no greater than they are with other e-mail services in general.[37]

After concluding that the use of Gmail does not violate an attorney's duty of confidentiality, the opinion draws an analogy between the commercial dimension that appears to be at the heart of the Gmail controversy and an attorney's use of external support services. The commercial dimension is the primary difference between Gmail's advertising service and other common software scanning methods, and it appears to be the source of much of the controversy. New York Code provides that a lawyer may not "knowingly. . . [u]se a confidence or secret of a client for the advantage of the lawyer or of a third person, unless the client consents after full disclosure."[38] According to the opinion, Gmail's advantage from the information, advertising profits, is not substantially different than the profits that lawyer services such as litigation support companies make.[39] This view is consistent with a recently published ABA opinion finding that it is acceptable to outsource technical support staff, so long as reasonable precautions are taken to ensure that sensitive information remains confidential.[40] In addition, the observation addresses the heart of the Gmail controversy: not that personal information is used for some malicious purpose to the detriment of the customer, but that Gmail is making a profit from it.

The opinion has several implications for the activities of attorneys and the general acceptance of technology by the legal community. First, it makes attorneys' jobs easier by allowing them to use the third largest e-mail provider. Second, the opinion avoids presenting a threat to other automated scanning tools used by e-mail providers. The primary difference between Gmail's scanning and anti-virus scanning is the marketing purpose. The marketing purpose has no realistic impact on confidentiality, so an opinion invalidating the use of Gmail would also cast doubt on other automated scanning tools. And finally, the

---

[37] *Id.*

[38] N.Y. Code DR 4-101(B)(3).

[39] N.Y. Ethics Op. 820 (2008).

[40] ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 08-451 (2008). The opinion also states that the client's informed consent is required if their confidential information will be revealed to the technical support staff.

success of Gmail's service suggests that other similar advertising models will come into existence in the future. As technology and advertising models continue to evolve, companies will probably come up with new ways to generate profit from similar targeted advertisements. These business models do not threaten confidentiality as long as humans are not exposed to the information used to generate the advertisements. This opinion helps to pave the way to the immediate acceptance of more business models like Gmail.

CONCLUSION

Like many new communications technologies, Gmail was controversial when first introduced due to privacy and security concerns. State bars reflected this reluctance to trust the security of a new communication technology by initially proscribing the use of e-mail to transmit client confidences. But after several years of using and becoming familiar with various e-mail services, the legal community is beginning to accept the risks associated with online data storage and mechanized scanning technology. Following these developments, the first state bar opinion to address the confidentiality of Gmail concluded that it does not pose a greater risk than e-mail generally. The New York State Bar's opinion has positive implications for attorneys and technology, and should provide guidance to other states that consider this issue.