



# ELECTRONIC COMMERCE & LAW

VOL. 14, NO. 42

**REPORT**

NOVEMBER 4, 2009

## INFORMATION AGE CONTRACTING

It is past time to update contract boilerplate so that it will work in the information age. Traditional boilerplate used by in-house and outside counsel has stood the test of time, but times have irrevocably changed. Boilerplate needs an overhaul and this article looks at why and provides examples.

### Modern Contracts: Boilerplate Needs an Overhaul for the Information Economy

By HOLLY K. TOWLE

**“B**oilerplate” language or clauses are “standard” text tending to be used repeatedly without change. The term stems from printing presses. Thick sheets of steel (suitable for steel boilers) were used for text of standard ads and syndicated columns. Today, “boilerplate” is stored in computers and, unlike the steel plates, can easily be changed.

Regardless, many lawyers continue to assume that boilerplate written for a vanished economy and tangible items still works, or they hesitate to change boilerplate from fear of destroying language necessary to a forgotten legal nuance. However, much boilerplate needs change to work in our computer based, information economy. For example:

- An insurance company negotiating a “cloud computing” paper contract to access online storage of critical records probably assumes that the signed paper contract is the governing document and, based upon it,

the company will provide passwords to employees with authorized access. If those employees click “I Agree” to contradictory terms of use appearing on the log-in screen, do those terms vitiate, amend, or supplement the signed paper contract or may they be ignored? Traditional boilerplate will not answer that question, but traditional “amendment” or “integration” clauses could be updated to do so.

- A buyer of a distressed company will use its tried and true acquisition agreement that might, or might not, have been updated to use language capturing all modern property types, including intellectual property. But has that “boilerplate” been updated to cover licenses of information that is not “intellectual property” or even “property”? Have the boilerplate due diligence checklists and seller representations and warranties been updated to address information age liabilities such as unreported data security breaches or customer lists with names that may not be used because of “opt-outs” from e-mailings?

It is time to change boilerplate to catch up with information age issues. The need to do so has been around for over a decade, but boilerplate continues to lag. To get the ball rolling, this article contains an illustrative list of typical boilerplate clauses that are candidates for reconsideration.

#### ‘Written’

Contracts are replete with mandates to provide “written” notice or documentation. Notice of default, amendment, waiver, and assignment are often slated to be accomplished by “written notice” or a “signed writing.”

*Holly K. Towle is a partner with K&L Gates LLP, an international law firm, and the cross-firm coordinator of the firm’s e-Merging Commerce group. Holly is located in the firm’s Seattle office and is the author of The Law of Electronic Commercial Transactions (2003-2009, A.S. Pratt & Sons). Ms. Towle may be contacted via e-mail to Holly.Towle@KLGates.com.*

However, since the passage of the federal E-Sign Act in 2001<sup>1</sup> or similar laws in other countries, “writing” has included anything that can be captured in a paper or electronic record, i.e., essentially anything but oral communications. Thus, when parties require something in writing, what do they intend: paper or electronic? The question at the store is “paper or plastic”: the question for modern boilerplate is “paper or electronic”? Currently, the general (but not only) legal background rule is that “writing” means the parties want a record<sup>2</sup>—that record can be paper or electronic unless the contract otherwise provides.

The answer to “paper or electronic” depends upon the subject matter and party preferences. If the item is a notice of default, most parties want paper and delivery to a department staffed with a human being who can timely receive and read the notice, as opposed to delivery to an e-mail box that may have expired or whose owner is on vacation. If the item is notice of a five minute processing delay, e-mail may better serve minute-by-minute needs. The fix is to say what is intended, e.g., “Notice of default must be given in a non-electronic record or by facsimile; notice of [X] may be given in an electronic record by [e-mail][short message service][Twitter][?], in each case to the corresponding address for notices shown in § Y.” Note that simply allowing “electronic records” creates an ever-expanding universe, so it is best to specify which kinds of electronic media are acceptable.

The above assumes the parties are free to answer the question (“paper or electronic”) any way they like. However, sometimes a law forces the answer. For example, E-Sign only allows a party required to deliver a paper consumer disclosure (such as a consumer Truth-in-Lending Act disclosure) to substitute an electronic disclosure, *if* the disclosing party *first* provides a *different* disclosure about electronics and also obtains the consumer’s consent for the substitution.<sup>3</sup> In states with the Uniform Electronic Transactions Act (UETA), which is most states, if a law requires that a record be posted, displayed, sent, or communicated by a particular method or manner, or if a law requires a notice to contain information formatted in a certain manner, those legal rules still must be met even if electronics can be used.<sup>4</sup> This can literally lead to some bizarre UETA results (such as mailing an electronic CD by first class mail<sup>5</sup>), which cannot be varied by contract. E-Sign preempts some, but not all of UETA’s excesses, so it is best to get to know UETA and vary it by contract when possible.

A variation on the “writing” theme is statutes that do not use the word “writing” but merely require some-

thing to be “sent,” “delivered,” “received,” “made available,” or be in a form that a party “may keep.” Those kinds of statutes trigger a need to review boilerplate, e.g., if the contract says X will be “delivered,” merely posting X online may fail that requirement but meet a “make available” requirement. The boilerplate may need revision to achieve the desired result.

## Signatures

Boilerplate often requires a “signed writing,” such as for a contract or notice of cancellation. Typically, the requirement is intended either to meet a statute of frauds or to impose a formality to ward off contract formation or amendment by “too-casual” acts. Safeguarding against such acts takes more thought in modern commerce because “writings” are not just on “formal” paper: electronic writings include a range of options (e.g., e-mails, Twitter messages, short text messages and social network site messaging). Some voice-mails<sup>6</sup> can create a record, and some signatures can include recorded oral signatures or e-mail or other headers showing the name of the sending party or that party’s adopted alias. This is not a new concept— a paper letterhead has long been able to count as a signature if provided with required intent, and so have e-records.

In short, when the word “signed” appears in an agreement post E-Sign, it really means “signed, electronically or manually.” Accordingly, thought should be given to what *kind* of electronic “signatures” are legally allowed and which of those the parties desire to require or allow. This time the base question is “electronic or manual,” and sub-questions are “*which* electronics?” E-Sign defines “electronic” as “relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities,”<sup>7</sup> and an “electronic signature” as “an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.”<sup>8</sup> Intent continues to be key but there are more ways to sign and modern boilerplate should address which are acceptable. See also, “I Agree; Icons.”

Some approaches to this or other methods of contract formation focus on use of boilerplate e-mail logos or footers stating that the e-mail does not form a contract. Such a logo can be helpful and a good use of rules in UETA but, alone, will not necessarily defeat counter-arguments.<sup>9</sup> Further, there is no room for that logo in all media (e.g., Twitter), yet employees are using other media in ways that can make, and unmake, contracts. Here, training, not boilerplate, may be necessary.

## Amendments

As noted, some e-exchanges can count as signed writings and this is particularly dangerous for “amendments.” The parties may think they have precluded casual exchanges from amending a contract by requiring a “signed writing,” but an e-mail or other e-exchange can be just that. So which, if any, of those exchanges

<sup>1</sup> Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001 et seq.

<sup>2</sup> Under E-Sign, a record is: “information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.” Id. at § 7006 (9).

<sup>3</sup> See Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transactions* at Chapters 11.09 (2003-2009 A.S. Pratt & Sons).

<sup>4</sup> See UETA § 8(b).

<sup>5</sup> This particular UETA rule was rejected by Section 102(c) of E-Sign which provides that even if states adopt a specified version of UETA to escape federal preemption, those states may not circumvent E-Sign through “the imposition of non-electronic delivery methods under section 8(b)(2)” of UETA.

<sup>6</sup> E-Sign restricts some recorded oral communications from counting as an electronic record for purposes of an E-Sign consumer rule, for example.

<sup>7</sup> 15 U.S.C. § 7006(2).

<sup>8</sup> Id. at (5).

<sup>9</sup> See, e.g., discussion in *The Law of Electronic Commercial Transactions* at Chapter 13.08, *supra*.

should count as an amendment: a signed e-mail (or Twitter or SMS); an amendment agreed to online to an offline contract; terms of use contradicting but allowing access pursuant to a contract made offline? *Who* must sign: a particular level of officer (e.g., president) or any of the many employees who deal with counterparties daily? If the latter, e-mails and other messaging media, voice-mails and online contracts are particularly risky because of the number and informality of exchanges and the tendency of some business users to “click-to-agree” in an online session without checking the base contract. Some of this can be handled with training and some by contract. For example, a “master” contract can set the rules for amendments. For contracts subject to the common law, that law can create enforcement difficulties<sup>10</sup>—but as a starting point, updated boilerplate should at least attempt to set the baseline.

### Attribution

The Achilles Heel of electronic commerce is knowing who the contracting parties are, i.e., who clicked or signed electronically. This question encompasses *who* signed and whether they had authority to do so. The new e-laws largely do not answer these questions. Answers are left to the parties, although a new trend is to remove from parties the ability to accept the risk of *not* knowing with whom they are dealing.<sup>11</sup> Traditional boilerplate does not deal with this issue because in a face-to-face world, identification can be checked, and in a mail-order world a manual signature has self-authenticating features. But as the cartoon about the dog sitting at the computer says, “On the internet, no one knows you’re a dog.”

Boilerplate is not likely to solve this problem, but an “attribution” placeholder in boilerplate can act as a reminder of the need to deal with it and also to comply with laws dictating what can, or cannot, be done to authenticate counterparties. There is a plethora of law restricting what cannot be collected to authenticate individuals and imposing new liabilities for collection methods, use, storage and disposal; at the same time, there is developing law mandating that authentication somehow be accomplished despite such restrictions.<sup>12</sup>

Once a person is authenticated—that is, once you know you are dealing with John Doe—then the question will shift to whether John has the authority to act for John’s employer or other principal. This is a traditional agency law question but it can be harder to deal with in modern commerce because not as much is “apparent” under the agency law concept of “apparent authority” (e.g., either John or the dog could click the button). Boilerplate geared to particular contract types can set up a structure for approaching this issue. For example,

<sup>10</sup> See discussion of common law, which tends to ignore “written amendment only” clauses, and UCC and UCITA rules which tend to honor them, in *The Law of Electronic Commercial Transactions*, Chapter 13.08, *supra*.

<sup>11</sup> The FTC recently recommended to Congress that Congress develop national standards for identification and authentication and has also brought its first enforcement action for failing to provide adequate authentication. See e.g., “Security in Numbers \*\*\* \*\* SSNs and ID Theft”, FTC Report to Congress (Dec. 2008) (<http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf>).

<sup>12</sup> See, e.g., Holly K. Towle, “Personal Data as Toxic Waste: A Data Protection Conundrum,” *Privacy & Data Security Law Journal* at 504 (6/09) (AlexeSolutions, Inc.).

if the approach of a website service is to require its business customers to have a “primary administrator” who will decide what employees or agents of the business may use all or part of the site, then boilerplate documenting and allocating liabilities for that approach and risk allocations should be developed in accordance with applicable “attribution method” laws.<sup>13</sup>

### Notice Addresses

A way to make ambiguous a decision to require notices in a *non*-electronic record is to include an e-mail address in the “notices” section and then allow notices to be sent to *any* of the addresses shown there. What if the parties want to allow both paper and e-mail notices but want paper for the critical notices? A way to attack that conundrum can be to add a sentence to capture this concept (with more nuance): “E-mail may be used for day-to-day operations and contacts but not for a ‘notice’ or other communication required under this Agreement or by law.”

Whatever result is desired, boilerplate should not just say “e-mail.” Instead, it should specify the *type* of notices that can be sent to the e-address, e.g., “E-mail Address (for all communications, including legal).” Why? No one makes such a statement for postal addresses, so why do it for e-mail addresses?

The answer is in the UETA background rule. It says that an e-record is not “sent” unless it is directed to an e-mail address that the recipient “has designated or uses for the purpose of receiving electronic records or information of the type sent.”<sup>14</sup> The Official Comment says this: Many people have multiple e-mail addresses for different purposes. Subsection (b) assures that recipients can designate the e-mail address or system to be used in a particular transaction. For example, the recipient retains the ability to designate a home e-mail for personal matters, work e-mail for official business, or a separate organizational e-mail solely for the business purposes of that organization. If A sends B a notice at his home which relates to business, it may not be deemed received if B designated his business address as the sole address for business purposes. Whether actual knowledge upon seeing it at home would qualify as receipt is determined under the otherwise applicable substantive law.<sup>15</sup>

There are additional problems with UETA definitions of “send” and “receive” and a significant number of other UETA rules, some of which could be resolved with updated boilerplate.

### Personally Identifying Information

The law is increasingly protecting information that personally identifies a human being (personally identifiable information, or PII). The word “privacy” is used, but PII often is not private. To the contrary, it often includes information found in commerce, public records or the telephone book. Nevertheless, depending upon the source of the information and its type, there may be a law purporting to govern its collection, use, disclosure, storage, retention duration, transfer, disposal and so on. With that in mind, consider typical boilerplate that some parties assume will protect PII:

<sup>13</sup> Various laws include attribution method rules (e.g., UETA, UCC Article 4A and UCITA).

<sup>14</sup> See UETA § 15(a)(1)(1999 Uniform Version).

<sup>15</sup> *Id.* Official Comment No. 3.

The parties agree to safeguard all confidential information in the same manner as they safeguard trade secrets, except for information that is publicly disclosed through no fault of the disclosing party.

This boilerplate was drafted when only private or confidential information was legally protected—a concept that has died in modern commerce. A name and bank account number collected to debit a purchase or credit a paycheck are not “confidential” under the common law: they appear on checks sent through the stream of commerce. However, they are protected under data protection laws. They might not be covered by the above clause, however, because its scope is limited to “confidential” information.

What about the exception for public disclosure? It is too broad: data protection laws continue to apply regardless of whether the data becomes public—the information may still be sensitive or there is no literal end to the data protection duty. In contrast, there generally is no point in protecting a trade secret after it becomes public because the secrecy (and the trade secret status) is typically lost upon publication. The “no fault” concept in the above text is similarly too broad: duties under data protection laws tend to look to reasonable care or statutory allocations of liability, regardless of “fault.” Indeed, no one may be at fault: Both the holder of the information and the “data subject” may have acted without fault and both may be victims of a “hacker” or “identity thief.”

As for the safeguard duty, it is both too much and too little: Treating a name and bank account number like a trade secret can be too high a duty given that the information appears on circulating checks, whereas status as a trade secret is lost upon public disclosure. Trade secret safeguards can also be too low, e.g., locking up that information like a trade secret will not satisfy ACH debit rules requiring encryption of banking information.

Another problem with the clause is that it does not address what the parties must do if one experiences a data security breach. That circumstance is increasingly regulated under state, federal, and international data protection laws for personal information.<sup>16</sup> Although the new laws are not uniform, contemplation of their basic concepts in boilerplate should prove helpful, although no boilerplate clause will comply with every applicable privacy law and it is a pipedream to even hope to develop such a clause. Updated boilerplate clauses can, however, deal with some issues common to security breach notice laws.

### Integration or Merger Clauses

A typical integration or merger clause merges previous agreements concerning the same subject matter into one agreement. If getting to one final “purchase agreement” involved previous oral or written understandings, a merger clause supersedes them and says that the express provisions of the final purchase agreement constitutes the “entire agreement” of the parties as to particular subject matter. Nothing else is intended to count.

But that is not always the case in online commerce. A partial fix is to expand the list of items which actually

constitute the “entire agreement.” Candidates include, for example, log-in representations and warranties; website terms of use and certain disclosures; the privacy policy; linked terms; consents provided on the online path to checkout; codes of conduct; and so on. Failure to include the appropriate list of items might preclude their application<sup>17</sup> or cause a court to conclude that the merger clause was *not* intended to be the “entire” agreement. Note also that inclusion of terms that cannot later be proved, e.g., inclusion of incorporated terms posted online that have changed or disappeared by the time the “entire agreement” is offered to a court, can create proof problems. See No. 18.

### Force Majeure

“Greater force” or force majeure clauses excuse parties from not performing their contractual obligations due to unforeseen events beyond their control such as “acts of God” and war. Most of these clauses have been updated to deal with computer phenomena such as denial of service attacks and Internet outages. However, the new “computer event” language is often added without qualification for a basic premise of force majeure clauses, i.e., the assumption that a party’s failure to perform could not reasonably be avoided.

That kind of assumption can be expressly stated and expanded as appropriate. For example, a terrorist attack or war may, indeed, interrupt the ability of one party to access data held by the other on the internet. But before being excused from providing access, consider whether one or both parties should have established and maintained reasonable backup facilities and procedures.

### Incorporated Terms

Contracts have traditionally incorporated by reference terms contained in a separate physical document, e.g., depositors might sign a signature card incorporating by reference the deposit account agreement. Although incorporation remains a valid concept in modern commerce, there are a few twists when the incorporation is of documents posted on the internet. Why? For one thing, the person signing the contract incorporating the posted terms might or might not have a computer; the link to the terms might be stale; the posted terms might include internal links that are stale or so numerous and voluminous that a “copy” cannot be printed or saved reliably to meet E-Sign or UETA rules, or that will still work when the document must be submitted into evidence. The parties might not even be able to prove what the incorporated terms were at the time the contract was signed because of changes to or disappearance of the posted version. Because of these and other factors, modern decisions sometimes require strict compliance with incorporation doctrines and include modern twists.<sup>18</sup>

### Information

Traditional contract wording uses tangible property concepts. However, numerous items important in an information economy are not tangible and some are not

<sup>16</sup> For a discussion of statutes requiring notice of data security breaches, see *The Law of Electronic Commercial Transactions*, Chapter 16, *supra*.

<sup>17</sup> See, e.g., *A.V. v. iParadigms, Ltd. Liability Co.*, 2008 WL 728389 (E.D. Va. 2008).

<sup>18</sup> See, e.g., *Affinity Internet, Inc. v. Consolidated Credit Counseling Services, Inc.*, 920 So.2d 1286 (Fla.App. 2006).

even property.<sup>19</sup> This is not a new concept. When intellectual property rights became as or more important than brick and mortar assets, contract wording made the shift from focusing on tangible property—sales, leases, ownership, and title—to dealing with licenses and other intangible property rights. Yet vestiges of too-restrictive language remain even as to intellectual property rights. Even fewer contracts contain language that fully contemplates laws regarding “information,” or electronic information.<sup>20</sup> For example, many internet terms of use for a site providing only a service (such as access to an online database), disclaim implied warranties of merchantability, a warranty implied under Article 2 of the Uniform Commercial Code regarding transactions in and/or sales of goods. What “good” is being sold on that site? The contract properly is a service contract controlled not by the UCC but by the common law or, in Virginia and Maryland, the Uniform Computer Information Transactions Act (UCITA).<sup>21</sup> Given that, common law and UCITA rules should be addressed. UCITA allows certain UCC disclaimers to suffice and even if it did not, it still would be a good idea to include them: Many courts are not making informed decisions regarding what is a good, service, or information. The law is in chaos and that may call for boilerplate contemplating several possible outcomes.

Acquisition or merger agreements are fraught with outdated language. Consider use of a defined term “property” to cover all types of property. The problem is that not all modern assets are necessarily “property,” so a more generic term may be preferable. Domain names are an example: In some states they are not personal property, or at least not for purposes of in rem actions to seize them or for purposes of conversion.<sup>22</sup> A different problem is that sometimes a complete category of assets is omitted: “Intellectual property” does not cover information that is not intellectual property. Some agreements attempt to solve this by expressly defining “intellectual property” to include information that is not intellectual property, but that can create its own issues and also make drafting more difficult when it becomes necessary to treat the concepts separately. For example, if a contract contains a combined definition it may also contain a warranty that no intellectual property has been infringed. Does use of “infringed” impact warranty coverage of data that is not copyrightable but is covered by the combined definition? Such data arguably cannot be “infringed,” although clearly statements regarding it could be “breached.” For illustrative purposes only, a modern definition of items acquired in a merger agreement might look more like this (assuming further definition of the capitalized terms):

“Assets” means any and all now or hereafter existing: (1) real property, personal property, and all other types of property, contract rights, accounts and licenses, whether for tangible or intangible items; (2)

<sup>19</sup> See, e.g., *The Law of Electronic Commercial Transactions* at Chapter 7.07, *supra* (case law regarding domain names as seizable—or not—property).

<sup>20</sup> For a discussion of the conceptual differences attendant upon information, see *id.* at Chapter 8.01, *supra* (nature of an access contract and applicable law).

<sup>21</sup> For a discussion of this topic with respect to internet access contracts, see *id.* at Chapter 8.20.

<sup>22</sup> For cases and varying views, see *id.* at Chapter 7.01, *supra*.

intellectual property; (3) data, text, images, sounds, codes, computer programs, software, databases, mask works and the like and including collections and compilations of them (whether or not all or part of such is intellectual property) and all other information (collectively, “information”); (4) access or use rights; (5) rights in internet, worldwide web or similar addresses, uniform resource locators, domain names and the like and all applications and registrations therefor; and (6) other rights of every nature whatsoever of the [Seller] or in which [Seller] has rights, permissions, possession or control of any nature, all whether proprietary, real, personal, tangible, intangible or mixed. Nos. (3) through (5) are referenced herein as “Information Assets.”

### Nature of Restrictions

Boilerplate representations and warranties in an acquisition agreement often have the acquired company state that it is not in material breach of any “contract” and it has not committed or failed to perform any act that could become a default under a material “contract.” The change in modern commerce is that there are more non-contractual rights that need to be considered. There are privacy “policies” which may or may not be contracts or may be quasi contracts; there are critical notices or waivers that might fall short of being contracts or that are not intended to be contracts. For example, some open source software licenses state that a user may copy and make derivative works from the software as long as the user gives credit to the licensor—is this a contract or merely a notice or waiver of two copyright rights of the licensor?<sup>23</sup>

A similar development in modern commerce is that compliance with many of the new “electronics” laws is not *required* by law. However, there are material *consequences* if the law is ignored. Assume an acquirer is concerned that the target company’s electronic records meet federal criteria for e-records. A general representation that the target complies with all applicable law might not achieve the desired result because the relevant law does not *require* compliance. However, there are *consequences* for e-records not meeting the criteria, i.e., they may be rendered worthless. Expanding boilerplate to deal with both realities is worth considering.

### ‘I Agree’ Icons; Counterparts

In every jurisdiction there are laws voiding all or part of a contract if it is not “signed by the party to be bound.” “I Agree” buttons are becoming “boilerplate” contractual consent, but the question is whether they are *signatures*. The question here is not whether the signature can be electronic—that is fine in most (but not all) cases given the federal Electronic Signatures in Global and National Commerce Act, the Uniform Electronic Transactions Act, and other laws. However, that just means the signature can be *electronic*. The question here is whether there is a signature.

Some “I Agree” buttons are not necessarily “signatures,” although they are contractual consent.<sup>24</sup> If the contract requires a “signature,” modern “boilerplate” should include sufficient language to obtain one.

<sup>23</sup> For a discussion of this concept see *id.* at Chapter 8.03[2].

<sup>24</sup> See *id.* at Chapter 4.18[5](A Process Might Be a Signature in the United States).

Confused? Recall that most contracts can be formed with any manifestation of assent, e.g., the nod of a head, shaking hands, clicking a button or performing another act. Conceptually, all “I Agree” buttons will *form a contract*. The issue is whether that contract is a “signed” contract. To get a signature in modern commerce, consult current definitions.

For example, language in both E-Sign and UETA expands the concept of what may be a signature to include a “process.” The jury is still out on what that means but it at least means an encryption process creating a digital signature.<sup>25</sup> Consider the impact of the new process concept and the fact that “pages” of agreements are not necessarily signed anymore. Instead, a screen incorporating or referencing the agreement is signed. Now consider “counterpart” boilerplate. A typical “counterpart” clause says the agreement may be executed in two or more counterparts, all of which will be considered one agreement becoming effective when the last counterpart is signed and delivered. The language contemplates paper agreements or signature pages that can be bundled together—what is the electronic screen equivalent? The answer depends upon the format being used.

### Section Headings

Here is a typical boilerplate clause:

**Section Headings.** Section headings have been included in this Agreement merely for convenience of reference. They are not to be considered part of this Agreement.

This has never been quite true but the defect is exacerbated in electronic commerce. What these clauses likely mean is that the text of the section needs to prevail over the shorthand heading, but such clauses often go too far and say the heading is not part of the agreement at all. To the contrary, when a clause must be conspicuous, a traditional safe harbor under the Uniform Commercial Code Article 1 definition of “conspicuousness” has been a heading in all capital letters. Revised Article 1 (discussed below) changes the definition of “conspicuous,”<sup>26</sup> but still headings can be used to meet conspicuousness requirements, so why say a heading is not part of the agreement?

### Revised UCC Article 1

For years some boilerplate has been based on default rules in UCC Article 1. As of 2008, a majority of states had adopted a revised version of Article 1 which changes some of the assumed norms. For example, consider the duty of “good faith.” The revised version applies to both parties, including consumers, and is not limited to merchants. As for the definition, “old” Article 1 defined “good faith” as, essentially, honesty in fact. That means that a covered party<sup>27</sup> required to accept or decline in good faith, may be wrong in his conclusions as long as he is honest in fact.

However, under the revised uniform definition, “good faith means honesty in fact *and the observance*

*of reasonable commercial standards of fair dealing.* Given the ambiguities latent in that phrase and the often broad use of Article 1, as well as the lack of standards in many areas of commerce, boilerplate promises of good faith that assume the old definition should be reconsidered. It should be noted that not all states have accepted this change, which makes another point important: Revised UCC Article 1 is not uniform.

Critically, note that the default “governing law” rule for Revised Article 1 has not been adopted in any state—only in the U.S. Virgin Islands. No state was willing to enact the revised rule, which was akin to having governing law for the contract work like a pinball machine. Instead, states have retained the old version or adopted non-uniform versions. That makes the best of a bad situation but also creates a greater need to deal with choice of law by contract when possible.<sup>28</sup>

### Globalization

Boilerplate should be considered in light of operations in a global economy. For example, some countries will not recognize a U.S. choice of forum clause but in the United States, failure to specify a choice as “exclusive” can vitiate the choice.<sup>29</sup> If a contract contains that boilerplate wording, which can be a must in the United States, a remedy might be denied in countries not recognizing the choice. A choice can also have unintended consequences when data or other items are “outsourced” overseas and an injunction is needed to protect intellectual property or prevent disclosure of confidential or protected personal information—action in the chosen country might not be viable or timely enough to deal with the situation in the outsourced location. Here, boilerplate may need to give way to a more nuanced approach.

### Damages

Boilerplate damage provisions often shield one or both parties from consequential or similar damages. Parties typically view this as a good result and their hope is to shield one or both from lost profits and similar damages that are foreseeable, e.g., shielding a payment processor from lost profits of the retailer if the processor’s system goes down during a holiday buying season. However, in modern commerce these exclusions often need to be more nuanced, e.g., if the payment processor suffers a security breach of consumer credit card information, data security laws and payment industry standards expose the retailer to significant fines or damages, most of which will be consequential. In that kind of situation, the parties may wish to attempt to renegotiate the boilerplate.

### Books and Records; Audits

It is not unusual to see a clause like this: “During the Term and for a period of five (5) years following its termination, Company must keep all usual and proper books and records relating to its distribution of Product, including but not limited to, books and records related

<sup>25</sup> See *id.* at Chapter 4.05[3].

<sup>26</sup> See the Revised definition in 1-201(10). Under Revised Article 1, additional options to achieve conspicuousness such as marks or asterisks setting off text, might well come in a heading.

<sup>27</sup> The Article 1 definition does not apply to all articles. Some UCC articles already have the “newer” definition.

<sup>28</sup> For a discussion of the variances made by states to Revised UCC Article 1, see 2008 updated version of Keith A. Rowley, *The Often Imitated, But Not Yet Duplicated, Revised Uniform Commercial Code Article 1*, at 1A (originally printed as 38 U.C.C.L.J. 195 (2006)).

<sup>29</sup> See e.g., *The Law of Electronic Commercial Transactions* at Chapter 8.10[4], *supra*.

to marketing activities.” This kind of clause, however, is meaningless during the middle of our transition between paper and pixel-based commerce—nothing is usual any more, and promising to keep “proper” e-records can be too much for a routine promise (see “Electronic Records”). Further, not all records can or should be retained for the same time period: Some might contain personally identifying data that is subject to a different rule or that cannot be retained or viewed at all by the other party. As for audits, if one party expects to do electronic searches through the other’s records, that party should contract for retention in the desired form and within a defined scope. Importantly, any clause assuming or requiring “adequate” books and records may need to take into account special substantive, evidentiary and litigation discovery rules regarding electronic records.

### Electronic Records

The first wave of the transition from paper to electronic records answered the question: Must paper be used or may records be electronic? The answer is, generally, that electronic records can count, so contract boilerplate has less need to deal with that kind of issue (although the need has not entirely disappeared). The question receiving less attention is whether electronic records will be reliable enough to be used for traditional purposes satisfied by paper records such as for contract enforcement, litigation, audits and compliance. E-Sign literally allows the validity of an electronic record to be *denied* if E-Sign requirements are not met (the rule has not yet been construed by a court). As for evidentiary rules, one court enunciated the danger for litigation this way:

Be careful what you ask for, the saying goes, because you might actually get it. For the last several years there has been seemingly endless discussion of the rules regarding the discovery of electronically stored information (ESI). Very little has been written, however, about what is required to insure that ESI obtained during discovery is admissible into evidence at trial . . . . This is unfortunate, because considering the significant costs associated with discovery of ESI, it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence or rejected from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted.

...

[A]lthough “it may be better to be lucky than good,” as the saying goes, counsel would be wise not to test their luck unnecessarily. If it is critical to the success of your case to admit into evidence computer stored records, it would be prudent to plan to authenticate the record by the most rigorous standard that may be applied. If less is required, then luck was with you.<sup>30</sup>

Modern contracts should consider e-record laws and regulations and e-evidentiary rules. Discovery in litigation of those records must meet Federal Rules of Civil Procedure requirements for “electronically stored information.” And no, these rules are not really the same as rules for paper documents even if they look the same.<sup>31</sup> Some rules can also run counter to others and

will need special treatment, e.g., some data security laws require disposal of information when the purpose for which it was collected has been met,<sup>32</sup> yet the FRCP require retention when litigation is threatened. Some destruction clauses in boilerplate allow one party automatically to destroy information at the end of a contract, yet it may need to be held under ESI rules. The ability to meet U.S. discovery rules should also be considered when structuring activities of overseas branches or outsourcing in countries that will object to data transfers into the United States.

### Disposal & Transfer

Data or other information is often exchanged between parties and either returned or destroyed upon contract termination. For personally identifying information, the question is whether transfers and disposal are done in compliance with modern data protection laws regarding transmission and disposal of particular data types, including hardware containing it. Boilerplate should be revised to address at least the basics of these new restrictions.<sup>33</sup>

### Conclusion

The focus above is on the need to update traditional boilerplate for modern commerce. However, there is a next generation of boilerplate that could be included in information economy contracts. For example, the Federal Trade Commission and at least one state have started to define the kinds of baseline controls for electronic access to personally identifying information.<sup>34</sup> Laws such as the Federal Computer Fraud and Abuse Act criminalize and allow civil suits when access is unauthorized, or when authorized access is exceeded, and courts are split over what it means to exceed authorized access.<sup>35</sup> What does it really mean, then, when a contract says that a party may “access” an online service or particular areas of a database? Parties can spell that out each time or perhaps it is time to develop a boilerplate definition encompassing background law and issues the law inadequately addresses (subject, of course, to alteration as necessary per context).

There are myriad other issues to address in modern contracts.<sup>36</sup> Before dwelling on them, however, it seems

---

ter 4.03[6], *supra* (Admissibility and Reliability of Electronic Records).

<sup>32</sup> See original version of 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth [of Massachusetts] at 17.03(g) (limiting the time personal information is retained to that reasonably necessary to accomplish such purpose); the Commonwealth issued subsequent versions of this regulation because of heavy criticism. This time limitation no longer appears in the 2009 version which is effective in 2010 (see <http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>); the concept tends to appear most frequently in foreign data protection laws.

<sup>33</sup> For a discussion of these kinds of laws, see *The Law of Electronic Commercial Transactions* at Chapter 16.11 (transmission statutes) and Chapter 16.12 (disposal), *supra*.

<sup>34</sup> See e.g., *id.* Chapter 16.06[2].

<sup>35</sup> *Id.* at Chapter 3.05.

<sup>36</sup> For example, consider a traditional boilerplate representation and warranty in an acquisition agreement to the effect that the seller is qualified to do business in each jurisdiction in which it does business, a clause written when “doing business” registration or other requirements could be traced to physical locations or personnel. In an information age where a small business can be the corner drugstore to the world, either

<sup>30</sup> *Lorraine v. Markel American Ins. Co.*, 241 FRD 538-560 (D. Md. 2007).

<sup>31</sup> For a discussion of these and additional related issues, see *The Law of Electronic Commercial Transactions* at Chap-

best to address the still-lingering vestiges of boilerplate written for a goods economy conducted non-electronically. Contract law has always reflected the history of the United States economy.<sup>37</sup> Just as it was

---

because of its own website or sales through others (e.g., Amazon.com or eBay), what update to the representation is appropriate to address valid concerns of each party without straying into absurdities? As another example, consider whether standard employment applications, taken online or offline, have been updated to include a consent to transfer of personal data from countries requiring consent in this age of global employees and new data protections (or, alternatively, to prohibit applications from countries with data protection laws that reasonably cannot be met or are too expensive to meet).

<sup>37</sup> See Holly K. Towle, *The Politics Of Modern Licensing Law*, 36 *Hou. L. Rev.* 126, 136, note 39, quoting Professor Karl Llewellyn, the reporter for UCC Article 2 when first written:

“It is possible that there are fields of our law more fascinating than that of Sales, but I find the possibility difficult to credit. For packed into this small sector of the law is the course of our history over a century and a half, reflected with a range which the narrowness of the subject matter would seem off-hand to make impossible.

...  
 “Mercantile capitalism yields to industrial capitalism . . . industrial yields again to financial capitalism: and the dyewoods, cloves . . . and simple textiles . . . are pushed out of dominance by chemicals . . . ; you follow iron . . . ; you meet sewing machines sold to householders on the installment plan, you meet locomotives sold on the “same” plan to an equipment trust . . . ; you find “choses-in-action,” which means here stocks and bonds, excluded from the Uniform Sales Act. You wake up then to the fact that the throne your subject matter once occupied is overshadowed . . .

previously necessary to unhorse that law to make way for manufactured goods, it is past time to ungoods and electrify contract boilerplate to contemplate intellectual property, information and electronic commerce.

Such an exercise should not assume that contract law written for a non-electronic world will, or should, be applied exactly the same way to electronic realms. There are differences and failure to take them into account could push courts into directions viewed as desirable or not, depending upon one’s perspective. To illustrate, in *Douglas v. US Dist. Court for the Central Dist. of Cal.*,<sup>38</sup> the Ninth Circuit found unconscionable, a clause effectively requiring one party to check the web daily to see if contract amendments had been posted by the other party. This was a consumer case and the court’s hostility to arbitration clauses likely influenced the outcome. The point, however, is that when change notices were mailed to customers on paper, the issue of what kind of checking for changes customers should do did not exist. When notices are moved online, the question of appropriate delivery methods is more complex and one-size-fits-all answers usually will not suffice. Whatever the outcome, the exercise should prove worthwhile.

---

...  
 “Finally Sales, as the law of the very subject matter of business, sets forth the problems faced by law under the peculiar United States regime: galloping economic development together with a multiple jurisdictional scheme. I do not know where else to find these things displayed so vividly, and so knit into one.”

<sup>38</sup> *Douglas v. U.S. Dist. Court for the Central Dist. of Cal.*, 2007 WL 2069542 (9th Cir. 2007).