ARTICLE 2B AS LEGAL SOFTWARE FOR ELECTRONIC CONTRACTING—OPERATING SYSTEM OR TROJAN HORSE?

By A. Michael Froomkin †

ABSTRACT

The proposed draft of Article 2B of the Uniform Commercial Code can be thought of as akin to a complex computer software suite which seeks to dominate a market by offering all things to all people. The author suggests, however, that Article 2B's electronic contracting rules interoperate poorly with existing digital signature laws, and with some forms of electronic commerce. The author also questions whether Article 2B is the proper means to enact controversial rules that ordinarily would make consumers liable for fraudulent uses of their digital signatures by third parties. After considering Article 2B's potential interaction with existing digital signature laws, state consumer laws and liability rules, and the practices of Certificate Authorities, the author suggests that Article 2B still contains several bugs in its code and is therefore still not ready for adoption.

TABLE OF CONTENTS

---

† Professor of Law, University of Miami School of Law; B.A., 1982, Yale College; M.Phil., 1984, Cambridge University; J.D., 1987, Yale Law School. Internet: froomkin@law.tm. I would like to thank Caroline Bradley, Amy Boss, Bernie Cosell, Patrick Gudridge, Richard Hornbeck, Ray Nimmer, Adam Smith and Jane Winn for their helpful comments on earlier drafts. I am particularly grateful to Pam Samuelson and Mark Lemley for including me in this Symposium. The initial version of this paper was delivered in Berkeley in April, 1998; unless otherwise indicated, this version seeks to reflect legal and technical developments as of October 1, 1998. Research was supported by a Summer Research Grant from the University of Miami School of Law.

Online commerce is no longer a prediction; it is an economically significant reality,[1] so significant that online sales may well become the predominant means of selling consumer goods. Online distribution may also someday become the primary means of distributing software and other information. So far, online contracting generally has proceeded with surprisingly few legal crashes. Nevertheless, law reformers across the world are rolling out model laws to conform to what appear to be the new realities of Internet-based trade, and to facilitate the use of new technologies such as digital signatures. Proposed Uniform Commercial Code Article 2B—Licenses[2] now joins this bandwagon. In its desire to create a complete legal regime for the regulation of transactions in licenses for information products, and in particular software and databases, Article 2B proposes several provisions relating to the online purchase and delivery of information and other products.

Like software vendors, legal reformers have different styles. Some attempt to create sleek, narrowly targeted products that meet a single, sometimes modest, need. Others have a more ambitious agenda, and attempt to create the legal equivalent of the software suite: wholesale legal reforms that provide a solution to every imaginable legal problem. And if legal reformers are software vendors, then legislators are the institutional buyers of their products. Some jurisdictions seek out the newest and latest legal devices; others prefer to hang back and wait for version 2, or even 3.x, or '99, when maybe the worst bugs will have been ironed out.[3] Moreover, like large corporate buyers, legislators have widely varying understand-

---

1. *See generally* UNITED STATES DEPARTMENT OF COMMERCE, THE EMERGING DIGITAL ECONOMY (1998), *available at* <http://www.ecommerce.gov/emerging.htm>.

2. U.C.C. Article 2B—Licenses (Aug. 1, 1998 Draft), *available at* <http://www.law.upenn.edu/library/ulc/ucc2/2b898.htm>. The Microsoft Word version of the August draft, available on the web site maintained by the University of Pennsylvania repository of U.C.C. drafts, contains redline and strikeout marks that show changes from the previous draft. To track changes from the April to the August draft one must acquire each of the intervening drafts available at <http://www.law.upenn.edu/library/ulc/ulc.htm#ucc2b>.

3. At the Berkeley symposium I learned that the Article 2B as software metaphor used in this paper, which grew out of a conversation with my colleague Patrick Gudridge, has been used by others, notably Cem Kaner. *See, e.g.*, Cem Kaner, *Bad Software—Who is Liable?*, Address at the Proceedings of the American Society for Quality's 52nd Annual Quality Congress (May 1998), *available at* <http://www.badsoftware.com/asqcirc.htm>; Cem Kaner, Brian Lawrence & Bob Johnson, *SPLAT! Requirements Bugs on the Information Superhighway*, 5 Software QA 18 (1997).

ings of the information products they are considering acquiring, and have different capacities to undertake whatever customization may be necessary to adapt a generic product to their environment. As a result of this diversity, current laws relating to online contracting and especially digital signatures are something of a patchwork, but they are evolving quickly.

As regards electronic commerce ("e-commerce") at least, Article 2B is also evolving rapidly. For example, in the five months between the March, 1998 draft,[4] (which was current when most contributions to this symposium first were being drafted) and the August 1, 1998 draft, provisions regarding e-commerce have been materially altered, and in one critical case completely reversed.[5] Substantial changes have appeared since the April 1, 1998 draft—which the drafters said was all but final. Subsequent changes resulting in versions dated July 1998[6] and August 1998 testify to the hard work of the drafters and to their attempts, perhaps not always successful, to respond to critics. No good deed goes unpunished, however, and when faced with so many continuous changes in a long and complex document, one is entitled—even required—to ask whether the code is stable and whether one can rely on it.[7]

---

4. U.C.C. Article 2B—Licenses (Mar. 1998 Draft), *available at* <http://www.law.upenn.edu/library/ulc/ucc2/2b398.htm>.

5. *Compare* U.C.C. § 2B-104(c) (Apr. 15, 1998 Draft) ("A statute authorizing electronic or digital signatures in effect on the effective date of this article is not affected by this article"), *available at* <http://www.law.upenn.edu/library/ulc/ucc2/2b498.htm>, *with* U.C.C. § 2B-104(c) (Mar. 1998 Draft), *available at* <http://www.law.upenn.edu/library/ulc/ucc2/2b398.htm> ("A statute authorizing electronic or digital signatures in effect on the effective date of this article is not affected by this article, *but in the case of a conflict this article controls.*") (emphasis added). *See also infra* text accompanying note 40.

6. The July draft, which was prepared for the July 1998 meeting of the National Conference of Commissioners on Uniform State Laws, can be found at <http://www.law.upenn.edu/bll/ulc/ucc2b/ucc2bamg.htm>.

7. It should not need to be said, but it also follows from the rapid rate of change in a complex document that arguments in favor of Article 2B based on some form of notice and estoppel ("we discussed this issue two years ago—where were you?") deserve to be treated with derision. Alas, some of Article 2B's more exuberant proponents continue to make such arguments. *See, e.g.*, Memorandum from the Business Software Alliance et al. on Article 2B (July 15, 1988) ("One would expect ALI motions and votes to be circumspect and to give credence to the open forum of NCCUSL and the endless hours of discussion heard and considered by the Article 2B Drafting Committee. But they do not. [One] motion on standard form contracts seeks to overturn the delicate compromise reached by the Drafting Committee after untold hours of debate and consideration of alternative approaches. The motions on choice of law and choice of forum also ignore hours of discussion and compromise, as well as commercial realities and needs. We do

One reason why Article 2B has proven to be so difficult to get right is that the information technologies to which it would apply are themselves in a state of ferment. As many papers in this Symposium demonstrate, the task of defining licensing rules for information is difficult enough; adding in the task of defining distinct rules applicable to all electronic contracts of sale, or even just those electronic contracts licensing information, may make it impossible. But while information licensing agreements may present special legal issues and problems that require a particularized legal regime, it does not follow that they require their own *electronic* contracting regime as well—unless there is something special about the electronic sale of information licenses, or about information itself that distinguishes the formation and enforcement of online sales agreements from contracts relating to other online sales. Whether or not the case for distinct rules relating to information licenses has been proved, the case for distinct rules relating to the electronic sale of information has not been made.

Indeed, to the extent that Article 2B creates unique electronic contracting rules, the introduction of special rules in Article 2B threatens to create confusion rather than standardization. When transactions are "mixed," combining information licenses with more traditional goods, the confusion may become more pronounced if inconsistent rules apply to different parts of the same transaction, or because the dominance of one set of rules provides unexpected outcomes. In any case, the over-ambitious reach of Article 2B seems certain to have unwanted and no doubt unintended consequences for e-commerce.

Although the electronic contracting provisions in Article 2B raise a host of interesting and complex issues, this Comment will give disproportionate emphasis to Article 2B's potentially awkward interaction with so-called digital signature laws, and with rules relating to Certification Authorities. Article 2B itself seeks to be technology neutral, and thus its e-commerce provisions apply more broadly than this Comment's focus on digital signatures might suggest.[8] Nevertheless, I chose to focus primarily on digital signatures because they are currently the most widely recognized method of electronic authentication, and are increasingly widely deployed. In addition, the profusion of laws and proposals relating to digital signatures at the state, federal, and international level means that, for this type of e-commerce at least, Article 2B does not enjoy the luxury of writing on a blank slate.

---

not support this type of above-the-fray tinkering, particularly on such fundamental issues."), *available at* <http://www.2Bguide.com/docs/amemo981.html>.

8. For instance, Article 2B also has innovative features regarding automated contracts formed by electronic agents, some of which are discussed in section II.D.

The diversity of existing and proposed approaches increases the case for standardization across jurisdictions. On the other hand, an evaluation of the standardization Article 2B offers must also take account of the policy choices embedded in the standard, and the extent to which it either affects other types of e-commerce or it risks creating dual and perhaps conflicting rules for electronic contracting depending on the subject matter of the transaction. Like the makers of a new operating system or a complex software suite, the proponents of a wide-ranging legal reform must contend with legacy applications and with the habits they have engendered. Despite some improvements in its most recent revisions, and even discounting for the relative newness of digital signature-based commerce and the laws that seek to enable it, there is ample reason to doubt that Article 2B is compatible with the emerging model of digital signature-based e-commerce.

I. BACKGROUND: DIGITAL SIGNATURES, CERTIFICATE AUTHORITIES AND THE EMERGING LEGAL LANDSCAPE

A digital signature is a mathematically generated, probabilistically unique, data string that can be associated with digitized information in order to demonstrate the authenticity of that information and the identity of the signer. A digital signature created with Alice's private key[9] links her to the data and can be used to prove that the data has not been altered since Alice signed it.[10] Anyone who has Alice's public key corresponding to the private key she used to generate the signature, and the right software, can then verify[11] the integrity of Alice's signature. Because the signature algo-

9. For a fuller explanation of public-private key technology see A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 50-53 (1996), *available at* <http://www.law.miami.edu/~froomkin/articles/trusted.htm>.

10. When combined with a digital time stamp the message can also be proved to have been sent at a certain time. *See id.* at 65-67.

11. Article 2B does not use the term "verify" in the context of electronic contracting. The term is used in the ABA Digital Signature Guidelines and in the Utah Digital Signature Act: "Verify a digital signature" means, in relation to a given digital signature, message, and public, key, to determine accurately that: (a) the digital signature was created by the private key corresponding to the public key; and (b) the message has not been altered since its digital signature was created. *See* DIGITAL SIGNATURE GUIDELINES § 1.37 (1996), *available at* <http://www.abanet.org/scitech/ec/isc/dsgfree.html>; Utah Digital Signature Act § 103(37), UTAH CODE ANN. tit. 46, ch. 3 (1995). Instead, Article 2B uses the term "authenticate" which refers to both the act of creating the original digital signature and the act of confirming its authenticity and validity. *See* U.C.C. § 2B-102(a)(3) (Aug. 1, 1998 Draft). Conflating the two significantly different actions into one term creates a real, and avoidable, potential for confusion.

rithm uses the entire original digitized information as input, if the information is altered in even the slightest way, the signature will not decrypt properly, thus showing that the message was altered in transit or that the signature was forged by copying it from a different message.[12] A digital signature copied from one message has an infinitesimal chance of successfully authenticating any other message.[13]

A digital signature cannot work well in isolation. In most arms-length uses where the parties have no other means of confirming their identity and the security of their signatures, and especially those involving the transfer of value, a digital signature requires a certificate issued by someone other than the parties to back it up. If Alice e-mails Bob a program that she has authenticated with a digital signature, the presence of the digital signature alone adds little. Bob needs a copy of the public key that corresponds to Alice's private key to check the validity of the signature. More importantly, Bob needs a way to confirm that the corresponding public key is actually Alice's and not an imposter's. Current practice—which may be about to change[14]—further assumes that before relying on Alice's digital signature, Bob usually needs to confirm that Alice's key is still valid, since keys are sometimes revoked before their natural expiry date due to key compromise or for other reasons.

In order to rely on the authenticity of Alice's public key, therefore, Bob needs to get the key, or data authenticating the key, from some source

---

12. Digital signatures achieve this by computing a *one-way hash value* of the message and then encrypting the hash value with the user's private key. A hash function takes an input string and converts it to a fixed-size, and usually smaller, output string. A one-way hash function adds the property that while it is easy to compute the hash value from the input it is very hard to find other inputs that produce the same hash output. *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 28 (2nd ed. 1996). The recipient checks the digital signature by decrypting the hash value with the sender's public key, then comparing the hash value with the independently generated hash value of the file received. If the two numbers are the same, the file is authentic and unchanged. *See* RSA Laboratories, *Answers to Frequently Asked Questions About Today's Cryptography* § 2.1.6 (visited Nov. 9, 1998) <http://www.rsa.com/rsalabs/newfaq/alg_tech.htm>.

13. *See* SCHNEIER, *supra* note 12, at 38 (noting that a digital signature using a 160-bit hash number has only a one in 2^{160} chance of mistakenly authenticating another document).

14. *See* Ronald L. Rivest, *Can We Eliminate Certificate Revocation Lists?*, PROC. OF FINANCIAL CRYPTOGRAPHY 178 (Rafael Hirschfeld ed., 1988) (proposing and advocating a means of dispensing with certificate revocation lists in which the proponent of a digital signature bears the burden of providing a suitably recent and reliable certificate to the relying party), *available at* <http://theory.lcs.mit.edu/~rivest/revocation.ps>; *see also* Richard Hornbeck, *The Troubling Truth About "Trust" on the Internet*, 10 J. ELECTRONIC COMM. 59, 65 (1997) (critiquing CRL model), *available at* <http://www.primenet.com/~hornbeck/trust.htm>.

other than the "Alice" sending him the original e-mail message. This is because if someone is forging a message from Alice, that malicious third party will send his own public key as well, claiming that it is actually Alice's. This imposture will fail if and only if Bob has access to Alice's real public key from some outside source, so that when Bob attempts to use Alice's real public key to verify a message signed with the imposter's private key, the verification will fail, revealing the forgery.

There are many ways of providing Bob with the information he needs to satisfy himself that the public key he will use to verify the authenticity of Alice's message is both genuine and still valid. One possible outside source is a business that sells and administers certificates attesting to the binding between Alice and her public key, and which offers online verification services. These businesses are known as *Certificate Authorities* ("CAs"). An increasing number of enterprises are seeking to establish themselves as CAs. Firms such as VeriSign offer a variety of CA services to all comers at a variety of prices and levels of assurance.[15] Others, such as the American Bankers Association (which recently announced an agreement with Zions National Bank in Utah to provide root CA services for banks), seek to serve specialty markets.[16]

The growth in the number of CAs, and the increasing interest in digital signatures as elements of e-commerce, parallels an extraordinary lawmaking effort on the part of state, federal, foreign, and international legislative and law reform bodies. Digital signature laws or policies have been debated, proposed, or adopted by almost every state in the union,[17] most European nations,[18] the EU itself,[19] UNCITRAL,[20] non-European na-

---

15. *See VeriSign Home Page* (visited Nov. 9, 1998) <http://www.verisign.com>.

16. *See ABA Announces Plan to Become Certificate Authority For Financial Services Industry* (Mar. 6, 1998) <http://www.aba.com/abatool/showme_rel.html?location=PR_030698ec.htm>; *OCC Approves A National Bank to Certify Digital Signatures* (Jan. 13, 1998) <http://www.occ.treas.gov/98Rellst.htm>.

17. For a continually updated summary of state legislation see McBride, Baker & Coles, *Summary Of Electronic Commerce And Digital Signature Legislation* (last modified Oct. 13, 1998) <http://www.mbc.com/ds_sum.html>.

18. *See generally* Juan Avellan, *Digital Signature Links*, (last modified June 10, 1997) <http://www.qmw.ac.uk/~tl6345/#Europe> (Summary of activities in European countries, including Germany, Italy and the UK.).

19. *See generally Towards A European Framework for Digital Signatures And Encryption*, COM(97)503, *available at* <http://www.ispo.cec.be/eif/policy/97503toc.html>.

20. *See generally Draft Uniform Rules on Electronic Commerce*, UNICITRAL, 32nd Sess., U.N. Doc. A/CN.9/WG.IV/WP.73 (1998), *available at* <http://www.un.or.at/uncitral/english/sessions/wg_ec/wp-73.htm>; *UNCITRAL Model Law on Electronic Commerce*, G.A. Res 51, U.N. GAOR 6th Comm., 85th plen. mtg.,

tions,[21] and many private bodies including the American Bar Association.[22] This activity responds to a real need: absent clarifying legislation, the law relating to CAs' duties and liabilities is likely to be confused and confusing.[23] Nevertheless, this outpouring of legislative enterprise was not caused by a barrage of lawsuits resulting from Internet commerce gone wrong.[24] Nor can this activity easily be explained by a massive pent-up consumer demand for digital signatures that has been held back by legal uncertainty, as there is only equivocal evidence of pent-up demand, and indeed only some evidence of demand pure and simple, on the part of consumers. The flurry of legislative activity appears primarily entrepreneurial, designed not only to facilitate existing demand for e-commerce but also to nurture new demand and speed the development of the necessary software tools and social institutions.[25] There is indeed some truth to one commentator's warning that, "[d]igital signature technology may be loved to death before it ever gets to really take off."[26]

Given the limited amount of Internet and other e-commerce that relies upon digital signatures today, both digital signature-based commerce and the statutes and rules designed to support it must be viewed as very early production models. If we are perhaps beyond the point of experiment and prototype and into the roll-out period, we are still at version 1.0[27]—and

---

U.N. Doc. A/51/628 (1996), *available at* <http://www.un.or.at/uncitral/english/texts/electcom/ml-ec.htm>.

21. *E.g.*, Japan. *See* Electronic Commerce Promotion Council of Japan, *Certification Authority Guidelines* (Alpha Version) (Apr. 7, 1997) <http://www.ecom.or.jp/eng/output/ca/eng-guideline.htm>.

22. *See generally* DIGITAL SIGNATURE GUIDELINES (1996), *available at* <http://www.abanet.org/scitech/ec/isc/dsgfree.html>.

23. I belabor this point in Froomkin, *supra* note 9.

24. So far as I am aware, there have been none, other than rare cases in which courts addressed whether an electronic "copy" can have the same legal force and effect as a traditional written signature in the absence of a "written original." *See, e.g.*, Allen v. Caldwell, 470 S.E.2d 696, 698 (Ga. App. 1996) (questioning the validity of a "facsimile" that lacks an "original").

25. It is entirely normal, appropriate, and often praiseworthy for the legislature (and others) to seek to enact power-conferring laws. *See generally* H.L.A. HART, THE CONCEPT OF LAW 27-33 (1961). The issue is the content of the facilities created for individuals to realize their wishes, and the structure of the resulting de facto as well as the de jure structures of rights and duties that will flourish within the coercive framework of the law.

26. Stewart A. Baker, *International Developments Affecting Digital Signatures*, (Oct. 1997) <http://www.steptoe.com/WebDoc.NSF/Law+&+The+Net+All/International+Developments+Affecting+Digital+ Signatures? OpenDocument>.

27. In the case of states such as Utah or Minnesota, which have already amended their original digital signature laws, we may be at version 1.1. The rapidity and frequency

every software user today knows what that means: like the early adopters of new software, the consumers and others who participate in the early days of digital signature-based e-commerce will be only a little more than uncompensated beta-testers. It is true that many of the legislative efforts today share common features, and in many cases were drafted by people who are in close communication.[28] On the other hand, there are also some sharp differences in approach regarding a number of issues, not least the allocation of risk and liability, the extent to which CAs or consumers should be shielded from loss, and the extent to which the relevant rules should be drafted by legislatures or regulatory authority delegated to administrative bodies.[29]

II. ARTICLE 2B ON ELECTRONIC CONTRACTING

While there is a great deal to be said for a uniform national standard regarding the legal force and effect of digital signatures and the regulation of CAs, we do not have enough transactional experience today to know which of the various approaches will be the best, whether we have a stable technological model,[30] or indeed whether any of these approaches already deployed might have unintended legal or social consequences. Article 2B's approach to e-commerce suffers from numerous problems as applied to digital signature-based commerce. First, as regards digital signatures, Article 2B is not uniform: different rules will apply in states with grandfathered digital signature laws. Second, whether or not states have preexisting digital signature laws, it will sometimes be difficult to figure out

---

with which digital signature laws are likely to be revised underlines the point that we are at an early stage in their development.

28. Several institutions enable continual contacts, including committees of the American Bar Association, the Commissioners on Uniform Laws, the UNCITRAL drafting process, and an excellent electronic mailing list with more than 150 members maintained by Professor Amelia Boss at Temple.

29. For an excellent survey of digital signature issues relating to other sections of the U.C.C., see Jane Kaufman Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TULANE L. REV. 1177 (1998). Very valuable, more narrowly focused, treatments of various issues relating to digital signatures and online sales or to digital signatures and specific articles of the U.C.C. include C. Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace*, 34 SAN DIEGO L. REV. 1225 (1997); C. Bradford Biddle, *Misplaced Priorities: the Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, 33 SAN DIEGO L. REV. 1143 (1996); Walter A. Effross, *The Legal Architecture of Virtual Stores: World Wide Web Sites and the Uniform Commercial Code*, 34 SAN DIEGO L. REV. 1263 (1997); and Jane Kaufman Winn, *Couriers Without Luggage: Negotiable Instruments and Digital Signatures*, 49 S. CAR. L. REV. 739 (1998).

30. *See supra* note 14 (noting a potential alternative model of e-commerce).

which parts of Article 2B apply to an e-commerce transaction. In particular, Article 2B applies its contract formation rules to so-called "mixed" transactions composed of matters covered by and excluded from Article 2B creating potential for confusion both as to what is covered and as to which parts of Article 2B constitute the contract formation rules. Third, Article 2B undertakes to override important parts of pre-existing consumer law in the interests of ease of use and national uniformity. Yet, the early deployment of new, poorly understood, and potentially fallible technologies such as digital signatures and especially intelligent agents seems to be an odd occasion for reducing consumer protections. Fourth, Article 2B adopts a liability regime for digital signature-based e-commerce that has been rejected by most states which have considered the issue.

A. Scope and Contract Formation

The first difficulty that confronts anyone seeking to understand the likely effects of Article 2B on e-commerce is determining the range of transactions likely to be affected by this Article. The very difficulty of this task is itself one of the more troubling aspects of Article 2B. Whether or not there already is too much legal uncertainty associated with e-commerce, the need for additional uncertainty appears to be remarkably low.

Certain parts of Article 2B have special application to electronic contracts, notably sections 2B-113 to 2B-120 (collectively within Part I.B, "Electronic Contracts: Generally") as well as Part 2 on contract formation, section 2B-107 on choice of law, section 2B-108 on choice of forum, and section 2B-111 on manifesting assent. All these provisions arise in the wake of Article 2B's scope provisions (sections 2B-103 to 2B-105), which set out the range of transactions to which Article 2B should be applied, and also discuss Article 2B's relationship to other law in the adopting state. As issues of scope and relationship are fundamental, they provide the starting point for an analysis of Article 2B's effects on e-commerce.

Section 2B-103(a) sets out what appears to be a quite limited reach for Article 2B: the Article will apply to (1) licenses, software contracts, and "access contracts,"[31] and (2) "any agreement to provide support for, maintain, or modify information related to a contract within the scope of this article."[32] But the treatment of mixed contracts is actually rather more

31. "'Access contract' means a contract to electronically obtain access to, or information in electronic form from, an information processing system. The term does not include a contract for physical access to a place, such as a theater or building." U.C.C. § 2B-102(a)(1) (Aug. 1, 1998 Draft).

32. *Id.* § 2B-103(a).

far-reaching and complex (and much changed, at least in presentation, from earlier versions of Article 2B). If Article 2B governs part of the transaction and other contract law governs part, then Article 2B will apply *inter alia* to information, informational rights and their documentation.[33] Article 2B will not apply to the conveyance of goods governed by Article 2 or 2A, unless those goods are licenses, software contracts, or access contracts, in which case Article 2B trumps 2 and 2A after all.[34] Furthermore, section 2B-103(b) applies the contract formation rules of Article 2B to all mixed transactions in which the parties agree to be bound by Article 2B.[35] Even absent agreement, the contract formation terms of Article 2B will apply to all mixed transactions involving services "or other subject matter" not within Articles 2, 2A, or 2B, if the "information or services that are within the scope of [Article 2B] are the predominant purpose of the transaction."[36]

Given the potentially wide reach of the contract formation terms of Article 2B, it becomes essential to determine which parts of that Article concern contract formation, and which are about something else. Alas, as Article 2B does not define precisely which sections concern contract formation there is room for confusion, both real and forensically feigned, as to what precisely constitutes a contract formation term for an electronic contract under Article 2B. The essence of a contract is agreement on its terms. Do rules about the terms of the contract constitute a contract formation term? Is a rule about choice of law terms or venue terms a rule of contract formation or interpretation and effect? Certainly all of Part 2 on

---

33. *See id.* § 2B-103(b).

34. According to section 2B-103(b)(2), Articles 2 or 2A also apply and Article 2B does not apply "as to subject matter that is excluded [from Article 2B] under Section 2B-104(3)," *i.e.* to the extent that a transaction:

> (3) is a sale or lease of a copy of a computer program as part of a sale or lease of goods that contain the computer program unless:
>
> (A) the goods are merely a copy of the program;
>
> (B) the goods are a computer or computer peripheral; or
>
> (C) giving the purchaser of the goods access to or use of the computer program is a material purpose of the transaction.

Id. § 2B-104(3) (emphasis added). This is not very clear. Is the purchase of a computer system, promoted as a word processing package and bundled with word processing software, for the express purpose of writing a book, a transaction in which "giving the purchaser ... access to or use of the computer program" is or is not "a material purpose of the transaction"? If it is, then unraveling the double negative of sections 2B-103(b)(2) and 2B-104(3)(C) suggests that Article 2B applies to the sale of the program and the computer system.

35. *Id.* § 2B-103(b)(3)(A).

36. *Id.* § 2B-103(b)(3)(B).

contract formation and terms falls within the contract formation rubric, but other parts would seem to also. For example, Part I.A ("General Terms and Scope") includes some sections that are part of contract formation, namely the definitions in section 2B-102, and the scope provisions in sections 2B-103 to 2B-105, discussed earlier, as well as sections that would not ordinarily be considered related to contract formation (e.g., section 2B-109 on breach of contract). Similarly, Part I.B ("Electronic Contracts: Generally") includes both rules of contract interpretation, (e.g., section 2B-115 "Effect of Imposing a Commercially Unreasonable Attribution Procedure"), and pure contract formation (e.g., section 2B-119 "Electronic Agents Operations").

A Reporter's Note suggests that the purpose of this language is to allow "maximum scope to the contract formation rules and electronic commerce."[37] Indeed, even if the exact reach of the contract formation terms cannot easily be discerned, it is evident that these terms will apply to a range of transactions well beyond pure software licenses or intellectual property licenses generally. Furthermore, if the parties agree, they can choose to apply Article 2B to any transaction that does not fall under either Article 2, or 2A—although in those cases, unlike those where Article 2B applies by its own terms, existing consumer law rules remain unaffected.[38]

B. Article 2B's Relationship to Existing Digital Signature Laws

One likely consequence of Article 2B's broad scope is that it will be applied to many agreements concerning the issuance and maintenance of digital signatures. Article 2B's effects on these transactions, as discussed in more detail below, are likely to be unanticipated and unhelpful. The potential for difficulties caused by Article 2B for purchasers and perhaps issuers of digital signatures contrasts with the less troubling approach adopted by the drafters of the Uniform Electronic Transactions Act ("UETA"). Article 2B and UETA originally shared a common general approach to the regulation of e-commerce, even if they differed on nomenclature. As the two drafting processes have proceeded, however, the documents have evolved in different directions. Despite some significant changes, Article 2B continues to take a relatively comprehensive and even intrusive approach, while UETA has scaled back to a less ambitious but perhaps more realistic strategy. Article 2B will affect everything from the formation of digital signature agreements to the assignment of liability if they go wrong. UETA now avoids the liability issue entirely.

---

37. *Id.* § 2B-103, Reporter's Note 5.
38. *Id.* § 2B-103(c)(1).

As of the April 15, 1998 draft of Article 2B—and in a sharp departure from the March 1998 draft—Article 2B provides a savings clause for pre-existing digital signature laws: "A statute authorizing electronic or digital signatures in effect on the effective date of this article is not affected by this article."[39] In contrast, earlier drafts of Article 2B had included the following italicized language: "A statute authorizing electronic or digital signatures in effect on the effective date of this article is not affected by this article, *but in the case of a conflict this article controls.*"[40] While this change is a welcome response to the complaint that Article 2B needlessly overturned existing state experiments in digital signature regulation, it introduces problems of its own. Grandfathering inevitably undermines uniformity, and thus undermines a major policy reason for even addressing the issue of digital signatures in an Article of the U.C.C. ostensibly devoted to licensing. Conversely, were Article 2B to be widely adopted, states with idiosyncratic digital signature laws would feel increasing pressure to repeal their laws and conform to the emerging national standard. The realities of national commerce mean that were Article 2B to be adopted, its digital signature provisions stand a good chance of becoming dominant; if so, the grandfathering of existing non-conforming state laws is less meaningful than it might seem.

As currently drafted, the digital signature provisions of Article 2B threaten to cause unneeded confusion. In Article 2B parlance, when Alice associates a digital signature based on her private key to any digitized information, be it an e-mail, a World Wide Web page, a purchase order, a program or a digitized movie, Alice *authenticates* that information.[41] Although earlier drafts of UETA used the term signature in a similar way,[42]

---

39. *Id.* § 2B-105(g). Note that this was section 104(c) in the April draft.

40. U.C.C. § 2B-104(c) (Mar. 1998 draft) (emphasis added).

41. Article 2B defines "Authenticate" as:

> to sign, or otherwise to execute or adopt a symbol or sound, or encrypt or similarly process a record in whole or part, with intent of the authenticating person to:
>
> (A) identify the person;
>
> (B) adopt or accept the terms or a particular term of a record that includes or is logically associated or linked with the authentication or to which a record containing the authentication refers; or
>
> (C) establish the integrity of the information in a record which includes or is logically associated or linked with the authentication or to which a record containing the authentication refers."

U.C.C. § 2B-102(a)(3) (Aug. 1, 1998 Draft).

42. *See, e.g.*, UNIFORM ELECTRONIC TRANSACTIONS ACT § 102(a)(20) (Mar. 23, 1998 Draft) (defining "signature" as "any symbol, sound, process, or encryption of a record in whole or in part, executed or adopted by a person or the person's electronic agent

the UETA drafters have now changed their approach. The September 18, 1988 UETA draft defines a signature as "an identifying symbol, sound, process, or encryption of a record in whole or in part, executed or adopted by a person, as part of a record."[43] The UETA formulation is now superior to Article 2B's. The term signature is more likely to be familiar to the average person than authentication, and therefore more clearly embodies the idea that legal consequences, such as the formation of contractual obligations, will tend to flow from certain uses of a digital signature. As discussed in more detail below, Article 2B's definition of authenticate obscures the difference between "authenticating" a document in the sense of showing it has not been altered and "signing" a document in the sense of completing a legal formality signifying an intent to be bound. If Bob appends a digital signature to a contract labeled "DRAFT," it often will be clear from the context that he intends only to demonstrate that it is his draft, and not to extend a firm offer. But there will inevitably be circumstances where the course of conduct makes it less clear whether a digital signature is associated to a document with the intent of authenticating or signing it.[44] Having one term do multiple duty risks confusion. A legal reform whose most immediate impact is that every risk-averse user of a digital signature for authentication must keep separate keys for each type of activity, and henceforth append a statement to message integrity authentications saying "this digital signature is only an authentication of the integrity of the message, it does not attest to the approval, acceptance or accuracy of the content nor does it constitute either an offer or an acceptance" seems to be the sort of modernization one can do without.

C. Article 2B Applied to CAs and the Conveyance of Certificates

Most models of digital signature-based commerce assume that some sort of trusted third parties, usually called Certificate Authorities (CAs), will provide essential intermediation services to participants in e-

---

with intent to: (A) identify that person; (B) adopt or accept a term or a record; or (C) establish the informational integrity of a record or term that contains the signature or to which a record containing the signature refers."), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/eta398.htm>.

43. UNIFORM ELECTRONIC TRANSACTIONS ACT § 102(a)(20) (Sept. 18, 1998 Draft), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/eta1098.htm>.

44. *See infra* text accompanying notes 87-89. *Compare* Guideline 1.4 of the ABA Digital Signature Guidelines, which defines "authentication" as: "A process used to ascertain the identity of a person or the integrity of specific information. For a message, authentication involves ascertaining its source and that it has not been modified or replaced in transit." This definition *excludes* signing with an intent to be bound. *See* DIGITAL SIGNATURE GUIDELINES § 5.2 (1996), *available at* <http://www.abanet.org/scitech/ec/isc/dsgfree.html>.

commerce. The drafters of Article 2B do not seem to have appreciated the extent to which Article 2B will apply not only to the users of digital signatures but also to the parties who may issue the certificates on which digital signature users must rely. Article 2B is likely to apply to the original provision of a certificate, and to the database services that make certificates reliable. Exactly when and to what extent Article 2B will apply is somewhat uncertain because it seems the drafters did not envision such highly customized transactions would nonetheless have mass market characteristics.

Imagine the following somewhat simplified set of related transactions. Alice, a merchant, intends to engage in e-commerce. As a first step, Alice contacts a CA in order to acquire one of the CA's digital certificates attesting to the linkage between Alice's public key and Alice's real-life identity. Bob, a consumer, contacts a different CA to acquire a certificate for his public key. The CAs may require some proof of ID, a payment, perhaps even some other form of security. Suppose Alice and Bob, neither of whom have any fraudulent designs, honestly provide everything required. If the CAs issue X.509-style certificates, currently the most common kind, the certificates will include several data elements, including a copy of Alice's public key signed by each CA's private key, a reliance limit, an expiration date, and a reference to the URL where each CA's *certification practice statement* (CPS) resides.[45] The CA's contract with its customers, and probably the certificates as well, will incorporate the CPS by reference.[46]

Suppose Bob visits Alice's web page and places an order for a computer program. If Alice's web site is signed with her private key, and if her certificate is compatible with Bob's browser, Bob can check the CA's *certificate revocation list* (CRL) to ensure that Alice's web page is truly hers, and not a spoof nor a hack.[47] Once reassured that Alice's key remains valid and uncompromised, Bob can send Alice his payment details with less fear that they will be going to a malicious third party pretending to be Alice.[48]

---

45. For a state-of-the-art CPS see *Verisign Certification Practice Statement* (May 15, 1997) <https://www.verisign.com/repository/CPS1.2/CPS1.2.pdf>.

46. *See generally* Froomkin, *supra* note 9, at 55-65, 97.

47. For an example of a CRL lookup form see VeriSign, *Verify the Status of a Digital ID*, (visited Nov. 19, 1998) <http://digitalid.verisign.com/status.htm>.

48. I have argued elsewhere that the second part of this scenario has some limits. If, for example, Bob is paying by credit card, the credit card company fulfills the role of trusted third party and there is little reason for Alice to require Bob to guild the lily with a certificate. Indeed, to the extent that the credit card company functions as an insurer,

If Alice is licensing information, with delivery online, she may be particularly interested in learning where Bob lives (as this may affect what law applies), and in making sure that Bob is who he says he is (as this may become relevant if he violates the terms of his license). Thus, if Alice requests Bob's public key and his certificate, she will want assurances that Bob's key remains valid and uncompromised. One way for Alice to confirm this is to consult the CA's CRL. If Bob's certificate checks out, Alice will complete the transaction.

It can be seen from the foregoing that in e-commerce models which rely on certificates verified by reference to a CRL, the CA is really providing two different things to Alice and Bob: 1) the certificate itself, and 2) access to a CRL. It is not an exaggeration to say that for these certificates, the CRL is at least as important as the original certificate.[49] The original, after all, will be generated only once; the CRL needs to be constantly available on a 24 hour a day, 7 day a week basis ("24x7"), and may be referenced any number of times by parties unknown at the time the certificate is created.[50]

1. Certification Services

Once Article 2B is enacted, CAs may find that its provisions allow them to structure the sale of certificates and certificate services in a manner that reduces their liabilities. The CA may structure the provision of a certificate as a sale, in which case Article 2 might apply absent other agreement. Subject to the doubts about the applicability of U.C.C. Article

---

there is little incentive for Bob to worry about the validity of Alice's public key either, since he bears little or no risk of loss. *See generally* Froomkin, *supra* note 9, at 68. Nevertheless, as the scenario in the text appears to animate most digital signature statutes, it remains worth considering.

49. Indeed, failure to consult a CRL before relying on a certificate in these models likely would be per se negligence. *See* DIGITAL SIGNATURE GUIDELINES § 5.4 (1996), *available at* <http://www.abanet.org/scitech/ec/isc/dsgfree.html>. A person who negligently uses an attribution procedure that *could* have been adequate may be estopped from pleading reliance upon the attribution procedure of which the certificate is a part, since only those who act reasonably are entitled to claim this type of reliance. *See, e.g.*, U.C.C.§ 2B-117(4) (Aug. 1, 1998 Draft) ("If the sender complies with the attribution procedure, but the receiving party does not, and the change or error would have been detected had the receiving party also complied, the sender is not bound by the error or change.").

50. On the other hand, one can also imagine alternate e-commerce models using digital signatures backed by certificates which do not rely on CRLs, perhaps because parties always demand reasonably fresh certificates, and the market responds by having CAs provide a continual stream of newly minted but short-lived certificates. This, more or less, is the model discussed in Rivest, *supra* note 14.

2 to intangible goods, this might work for the sale of the certificate alone, but it looks like a poor bet for the CA if the CA sells a package consisting of a certificate and CRL services:

> The view that a CA is providing a service (or a hybrid in which the service element predominates) appears more convincing than the alternative under either the "predominant factor" test or the "final product" test .... To issue a certificate worthy of trust, the CA must: (1) have a valid and verifiable certificate of its own; (2) conduct the inquiry on which the certificate will be based; (3) accurately state facts in the certificate, including both the facts about the subject and the facts about the CA's investigation; and (4) maintain a CRL. The CA's continuing duty to maintain the CRL in a form that can be rapidly and efficiently used by persons wishing to rely on a certificate is in itself significant evidence that the service element predominates in what the CA is selling.[51]

Even if the provision of the original certificate is an Article 2 sale, the provision of CRL services is unlikely to be a sale in most states. Indeed, states that use a predominant purpose test are unlikely to treat even the sale of the certificate as falling under Article 2. This legal vacuum will be readily filled by Article 2B.

If Article 2B is enacted, CAs may structure their deal as a license, in which case Article 2B would apply by default. In previous drafts of Article 2B it appeared that the provision of a certificate was excluded from Article 2B's definition of a "mass-market transaction," since each certificate is tailor-made for a customer and Article 2B's definition of a mass market transaction required that the information being licensed to each consumer be the "same information."[52] In contrast, the current draft defines a mass market transaction as including any "transaction within this article that is a consumer transaction,"[53] i.e., any transaction in which a

---

51. Froomkin, *supra* note 9, at 89-90.

52. For example, in the March 1998 draft, Article 2B defined a mass market transaction as a "consumer transaction ... directed to the general public ... for the same information." U.C.C. § 2B-102(a)(31) (Mar. 1998 Draft). The term excluded "a transaction in which the information is or becomes customized or otherwise specially prepared by the licensor for the licensee." *Id.* at § 2B-102(a)(31)(C). If a certificate is not the subject of a mass market transaction, by definition it cannot be covered by a "mass-market license" since a "'[m]ass-market license' means a standard form that is prepared for and used in a mass-market transaction." *Id.* § 2B-102(a)(30). As a result, various consumer protections designed to apply to mass market transactions would not have applied to CAs under the March 1998 formula.

53. U.C.C. § 2B-102(a)(32) (Aug. 1, 1998 Draft).

consumer[54] is the licensee.[55] Thus, under the current definition, a CA's provision of a certificate and CRL services to a consumer would be a mass market transaction, even though one suspects that the drafters' operating image of a consumer transaction remains one in which a person acquires a standardized program rather than a bespoke certificate.

As a result—unlike in previous drafts of Article 2B—the consumer protections in Article 2B that apply to mass market transactions[56] and licenses appear to apply to CAs that transact with consumers, although apparently not to CAs when they transact with other businesses. The Reporter's Notes conflict with this reading, however. For example, although section 2B-102(a)(32) defines a mass market transaction broadly, Reporter's Note 28 following that section cautions that the "definition must be applied in light of its intended function."[57] And, as in previous drafts of Article 2B, the consumer transactions envisaged are those in which every consumer acquires identical information, i.e., "relatively small dollar value, routine and anonymous transactions that occur in a retail market available to and used by the general public ... where information is made available in pre-packaged form under generally similar terms to the general public and in which the general public is a frequent participant."[58] This is a vision that would tend to exclude certificates, since every certificate must include the unique public key of the party being certified, and by their very nature few of these transactions will be anonymous. Worse, the same Reporter's Note states that the mass market transactions "concept applies only to information aimed at the general public as a whole, including consumers. It does not include products directed at a limited subgroup of the general public or restricted to members of an organization or to persons with a separate relationship to the information provider."[59] Perhaps this is merely a carry-over from earlier versions and will also be re-

54. "Consumer" is defined at section 2B-102(a)(10).

55. U.C.C. § 2B-102(a)(11) (Aug. 1, 1998 Draft).

56. The drafters identify the following as consumer protections in mass market transactions: "The provisions of this Article that provide additional consumer protections include: 2B-107 (choice of law); 2B-118 (electronic error); 2B-208 (limit on mass market license; right to refund); 2B-303 (limit on no-oral modification clause); 2B-304 (limit on modification of continuing contract); 2B-406 (warranty disclaimer); 2B-409 (third-party beneficiary); 2B-609 (perfect tender); 2B-619 (limit on hell and high water clauses); 2B-703 (exclusion of personal injury claim)." *Id.* § 2B-105, Reporter's Note 5.

To what extent each of these matter in the context of a CA is another debate; one place where it matters whether a transaction is mass market or not is the extent to which warranty disclaimers must be conspicuous. *See id.* § 2B-406 (b)(4).

57. *Id.* § 2B-102, Reporter's Note 28.

58. *Id.*

59. *Id.*

vised to match the changes in the definition, as otherwise it risks creating confusion.

One might also reasonably question whether the CA's provision of a certificate to a customer could alternately be considered the provision of an informational good within the purview of Article 2B. A certificate is certainly information, but it might be argued that in demanding and checking information about the subject of a certificate, the CA is performing a service whose predominant purpose is outside the scope of Article 2B, just as a lawyer or valuer who memorializes her professional opinion on paper or in an e-mail does not therefore fall within Article 2B's scope.[60] Whether a CA provides a professional service sufficiently like a lawyer or valuer to say that the memorialization is merely incident to the provision of a professional service is open to debate; conceivably it might turn on the quality or nature of the investigation or other initial inquiry performed by the CA.[61] This uncertainty is unhelpful.

In addition to controlling the form of the transaction, the CA has a number of options for manipulating the transaction's reality. A CA that chose to "sell" certificates could simply transmit the information to a client; a CA that wanted to emphasize the license or services nature of the transaction could ask clients to enter into a license agreement, by which the CA agrees to make the certificate available on a Web page to all who wish to see it. Current practice seems to be to convey certificates to customers. Verisign, for example, does not currently use license language to describe what happens when it creates a certificate for a consumer. This

---

60. *See id.* § 2B-104(5) (excluding contract for "personal or entertainment services"); *see id.* Reporter's Note 2.

61. *See* Froomkin, *supra* note 9, at 87-88:

> A certificate resembles a professional's opinion in that a certificate ordinarily is the tangible memorial of a process of analysis in which the subject's credentials were checked in some manner. On the other hand, a certificate differs from a professional's opinion in some ways that may be relevant. Any trustworthy CA will be managed by a professional—someone who knows how to run a trustworthy computer system—but it is not inevitable that the actual checking of credentials in all cases will be the sort of activity traditionally undertaken by professionals. If Alice's certificates are founded on checking the subject's passport, it may well be that the person who actually examines Alice's passport and issues her certificate is a clerk who has been trained in passport authentication, not an expert like a surveyor or valuer. There is no policy reason, however, why the classification of a certificate as a good or service should turn on whether the person making the report happens to be a professional.

Id.

may change. Already, both VeriSign's public keys and its CPS are made available to the public as licensed information.[62]

2. Provision of Access Services

While one might debate whether a CA's provision of a certificate falls within Article 2B, there seems far less doubt that the CA's provision of CRL services falls squarely within Article 2B's provisions relating to access to databases. The CRL is a database, and Bob's right to access it, or to point others towards it, is a license. This makes Bob's access to the CRL an access contract contemplated by Article 2B.[63] Furthermore, many of the parties consulting a CA's CRL are likely to be persons with no pre-existing contractual relationship with the CA. If Alice gets her certificate from a CA, Bob will need to consult its CRL whether or not he happens to have purchased anything from that CA. If the CA's provision of the certificate is not a license, (which seems to be current practice) but the provision of CRL services is, then either we have two separate transactions potentially governed by different rules, or one mixed transaction—parts of which may or may not be governed by different rules.

Before proceeding with the effect of treating a CA's business as involving a "mixed" transaction, one possible objection deserves to be noted. One might argue that a CA's services fall within the "core financial

---

62. "VeriSign public keys: VeriSign root public keys, including all PCA public keys, are the property of VeriSign, Inc. VeriSign licenses relying parties to use such keys only in conjunction with trustworthy hardware or software product in which the root public key is distributed with VeriSign's authority." *VeriSign CPS*, *supra* note 45, at § 12.13; *see also id.* at i (describing right to reproduce CPS itself in license terms).

63. *See, e.g.*, U.C.C. § 2B-102(a)(1) (Aug. 1, 1998 Draft) (defining "access contract" as "a contract to electronically obtain access to, or information in electronic form from, an information processing system. The term does not include a contract for physical access to a place, such as a theater or building."); *see also id.* § 2B-615 ("Access Contracts"). There are potential conflicts between some of the rules for access contracts, (e.g., section 2B-107(b) on choice of law for access contracts) which provides that even in a consumer transaction "[a]n access contract or a contract providing for electronic delivery of a copy is governed by the law of the jurisdiction in which the licensor is located when the agreement is made" and the general deference to digital signature laws in section 2B-105(g) since some state digital signature laws require that parts of their own law be applied regardless of the physical location of the CA. *See, e.g.*, Washington Electronic Authentication Act, WASH. REV. CODE § 19.34.220(3) (1997) (providing that CA must certify to "all those who reasonably rely on the information" that information in certificate and listed as confirmed is accurate, that subscribers accepted certificate; that all information foreseeably material to reliability of the certificate is stated or incorporated by reference in the certificate; and that CA complied with Authentication Act and other applicable laws of the state).

functions"[64] exceptions to Article 2B's scope. Article 2B does not apply "to the extent that a transaction ... provides access to, use, transfer, clearance, settlement, or processing of ... identifying, verifying, access-enabling, authorizing, or monitoring information" that is related to electronic cash, an "instrument," as defined in section 3-305, or the wholesale or retail transfer of funds including credit and debit card transactions.[65] Arguably the CA's contract with Alice to create a certificate is an agreement "that provides access to ... identifying, authenticating [or] ... authorizing information" that may well at some future date be "related to" electronic cash, or the retail transfer of funds. The problem, however, is that many certificates are and will be general-purpose identification certificates, and at the time Bob acquires the certificate neither he nor the CA may know what he intends to use it for. The time that a customer makes the agreement with the CA seems by far the most reasonable time to determine what law applies to the contract. Otherwise, this "core financial functions" exclusion might suddenly spring into effect if Bob one day used his certificate and Alice did a CRL lookup on it to support a transaction that involved electronic cash ("e-cash"). It seems more reasonable, therefore, to read the core financial functions exception in section 2B-104(4) as excluding the e-cash portion of every transaction in which e-cash is used, but not to every certificate.

If a CA's provision of a certificate and CRL services makes its deal with Alice and Bob a mixed transaction, it appears from the scope provisions of Article 2B that at least the contract formation parts of Article 2B will apply to the CA's relationships with Alice and Bob in the example above—even if the CA was able to categorize its provision of the original certificate as a sale of data rather than a license. Recall that according to section 2B-103(b)(3), even if the parties have made no agreement to invoke Article 2B, Article 2B's contract formation terms apply to the entire transaction if "the transaction involves services or other subject matter not within this article or Article 2 or Article 2A and the information or services that are within the scope of this article are the predominant purpose of the transaction."[66] "Services" is not a defined term in section 2B-102, and

64. U.C.C. § 2B-104, Reporter's Note 5 (Aug. 1, 1998 Draft).

65. *Id.* § 2B-104.

66. *Id.* § 2B-103(b)(3)(B). In addition, section 2B-103 (c) states that the parties may agree that all of Article 2B applies so long as this agreement does not alter mandatory consumer protections rules that would otherwise apply, and so long as this agreement does not remove a transaction from either U.C.C. Article 2 or U.C.C. Article 2A when one of those articles would otherwise apply. *See id.* § 2B-103(c).

the only other reference to services in section 2B-104 seems irrelevant.[67] If the term services is distinct from the sale of goods, as it is, for example, in U.C.C. Article 2,[68] but it includes the performance of an access contract, then section 2B-103 creates the risk of an anomalous situation: whether all of a transaction whose predominant purpose is the licensing of information would fall under Article 2B might depend on whether the transaction happened to include the provision of an incidental non-sale service.

Article 2B's reliance on Article 2's goods/services distinction is odd and slightly uncomfortable since a primary objective of Article 2B was supposed to be to erase that distinction. As Article 2B's Preface notes, the "distinction that used to be drawn between 'goods' and 'services' is meaningless, because so much of the value provided by the successful enterprise ... entails services [and information]."[69] Nevertheless, the current draft of Article 2B adopts the predominant purpose test[70] for determining when Article 2B should apply to a mixed transaction, [71] a test which will be familiar to U.C.C. lawyers from the context of Article 2. This is a substantial change from earlier versions of Article 2B: until recently, Article

---

67. Section 2B-104(5) states that 2B will not apply to the extent that an agreement "is a contract for personal or entertainment services by an individual or group of individuals, other than a contract of an independent contractor to develop, support, modify or maintain software." Interestingly, if somewhat puzzlingly, the Reporter's Note states that this exclusion "does not exclude situations where automation creates a digital replacement for activities previously characterized as personal services." *Id.* § 2B-104, Reporter's Note 6.

68. U.C.C. § 2-102 (1996) states that "unless the context otherwise requires, this Article applies to transactions in goods ...."

69. U.C.C. 2B, Preface, p.6 (Aug. 1, 1998 Draft) (quoting ROBERT REICH, THE WORK OF NATIONS 85-86 (1991)) (alterations in original).

70. On the "predominant purpose" test, see JAMES J. WHITE & ROBERT S. SUMMERS, UNIFORM COMMERCIAL CODE 3-4 (4th ed. 1995) ("If a sale of goods is not the 'predominant purpose,' then [the U.C.C. Article] does not apply at all.").

71. *See* U.C.C. § 2B-103, Reporter's Note 5:

> *Formation Rules.* Subsection (b)(3) addresses an effect created by Article 2B contract formation rules and the fact that Article 2B validates electronic commerce practices that may not be effective under common law or under current Article 2 or 2A. The subsection applies Article 2B formation rules to the entire transaction if Article 2B subject matter constitutes the predominant purpose of the transaction itself. This allows maximum scope to the contract formation rules and electronic commerce.

Id.

2B rejected the predominant purpose test in favor of a considerably more nebulous gravaman of the action test.[72]

3. *The Bottom Line: Effect of Article 2B on CA Transactions*

It follows from the above that Article 2B will confuse as much as it clarifies the legal duties and contractual rights of CAs and their customers.

In a state with no digital signature laws,[73] Article 2B will ensure that contracts for the licensing of information, and also mixed contracts that are formed via electronic contracting supported by properly implemented and deployed digital signatures, are as valid as contracts formed in a traditional fashion. Furthermore, in states that do not have pre-existing digital signature laws, or whose existing laws do not address contract formation or warranty issues, Article 2B is likely to have the following effects on contracts for the provision of a certificate and associated access to a CRL:

(1) If the conveyance of a certificate is a *license* of information within Article 2B, then both the certificate and the CRL lookup services are within all of Article 2B, since the CRL lookup service, an "access contract," is clearly covered by Article 2B.

(2) If the conveyance of a certificate is merely the *memorialization of a service*, akin to a lawyer's or valuer's opinion, then so long as the certificate relies on a CRL for its validity there is a good chance that the contract formation rules of Article 2B may apply to the entire transaction, since the initial certification service is a "service[] that [is] not within this article" and, arguably, "the information that is within this article"—the access to the CRL—is the predominant purpose of the transaction.[74] All of Article 2B applies to the customer's access to the

---

72. *See* U.C.C. § 2B-103, Reporter's Note 3 (Mar. 1998 draft) ("This Article applies *to the extent* that the transaction involves subject matter within its scope, but not to the extent that a particular subject matter or aspect of a relationship is excluded or otherwise outside the scope.") The tautological reassurance that what is excluded is excluded, and what is included is included was not comforting and seemed to mean that if the predominant purpose of the transaction is within Article 2B, then the contract formation rules—but not the other parts—of Article 2B applied to the entire transaction. Whatever it meant, we are well rid of it.

73. The situation in states with pre-existing digital signature laws may be even more complex. These statutes are not uniform, and Article 2B does not seek to displace them. *See* U.C.C. § 2B-105(g) (Aug. 1, 1998 Draft). To the extent that some of these statutes may have explicit contract formation terms, beyond defining a "writing," those terms will trump anything in 2B. *See id.* In the absence of an explicit provision to the contrary, however, Article 2B's terms will presumably control, including the treatment of mixed transactions described in this section.

74. *See id.* § 2B-103(b)(3)(B).

CRL, but only the contract formation rules apply to the initial generation and conveyance of the certificate, and to its updates.

(3) If the conveyance of the certificate is a *sale*, or if the CRL service is not the "predominant purpose" of the entire transaction, then different contract formation rules may apply to the certificate and the CRL even if they are acquired in a single transaction.

(4) If the conveyance of the certificate is *outside Article 2B* for any reason, and the certificate if of a type that does not require a CRL look-up to be valid, then Article 2B probably does not apply to the CA's part of the transaction.

Could not law *reform* come up with something more straightforward?

Moreover, the application of Article 2B to the CA's provision of CRL services threatens some odd results. CRLs online subject to Article 2B may be relieved of the burden of being constantly online and accessible. According to section 2B-615(a)(3), access pursuant to a contract that provides for continuous access,

> (3) must be available at times and in a manner:
>
> (A) conforming to the express terms of the contract; and
>
> (B) to the extent not expressly dealt with by the contract, in a manner and with a quality that is reasonable in light of the ordinary standards of the business, trade, or industry for the particular type of contract.

On the other hand, and of potentially greater relevance to most CA's provision of retail CRL lookup services, section 2B-615(b) provides:

> (b) In an access contract that gives the licensee a right of access at times substantially of its own choosing during agreed periods of time, an intermittent and occasional failure to have access available during those times is not a breach of contract if it is:
>
> (1) consistent with the express terms of the contract;
>
> (2) consistent with ordinary standards of the business, trade, or industry for the particular type of contract; or
>
> (3) caused by scheduled downtime, reasonable needs for maintenance, reasonable periods of equipment, software, or communications failure, or events reasonably beyond the licensor's control.[75]

There seems to be a conflict between the requirement in section 2B-615(a) that access conform to the express terms of the contract, and the

75. *Id.* § 2B-615.

terms of section 2B-615(b), which suggests that even when a contract provides for occasional access on a 24x7 basis, an intermittent and occasional failure of access is not necessarily a breach of contract. Every access contract for intermittent access drafted by a minimally competent lawyer is going to have some representation about the nature and quality of the service to be provided. Either the contract will promise uninterrupted 24x7 service, or the promise will be hedged with some sort of limitations. In contracts with any specific representation about quality of service, section 2B-615(b) becomes relevant only if the provider's express limitations are less sweeping than those set by Article 2B. Yet, in the absence of a more sweeping disclaimer, the subscriber would be entitled to think that the contract explicitly provides for a higher level of service. Perhaps section 2B-615(b) can best be understood as applying only to access contracts that have no agreed terms about quality of service at all. The text invites a broader reading,[76] but anything broader risks causing great confusion. Suppose that a CA promises "24-hour-a-day access to the CRL" or "best efforts for 24x7" or "access any time." Which of those make full-time access an express term of the contract? If a given formulation is an express promise of uninterrupted access, but a court finds that industry practice allows for substantial downtime, why should that norm be allowed to trump the express contractual term? At present, a CA's potential customers have almost no way of discerning industry norms, if indeed any have yet been born. As a result, there may be no norms for a CA to invoke; if there are, however, it is unclear why the CA should be allowed to do so if it has made any stronger contractual representations as to service reliability. Nor is it evident why lawyers should have to argue whether a blue screen of death[77] is a reasonable software failure rather than the unreasonable sort.

It may be that the computer technology backing up online services and especially the Internet generally remains sufficiently experimental and unreliable that providers need some sort of safe harbor provision to excuse unforeseeable breaches in service. Even so, the solution is to craft a stan-

---

76. The word "or" at the end of section 2B-615(b)(2) suggests that one should read an "or" into the end of section 2B-615(b)(1) and that therefore each of the three circumstances listed in section 2B-615(b) are independent defenses against claims for breach of contract.

77. The Free On-Line Dictionary of Computing defines the "blue screen of death" as "[t]he infamous white-on-blue text screen which appears when Microsoft Windows crashes. BSOD is mostly seen on the 16-bit systems such as Windows 3.1, but also on Windows 95 and ... Windows NT 4." Free On-Line Dictionary of Computing, *Blue Screen of Death* (Sept. 9, 1998) <http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?blue+screen+of+death>.

dard from contract language that allows providers to distinguish between regular service and premium. Not only should the language itself put a reader on notice that the ordinary 24x7 promise may mean less than it seems, but a CA which chooses to make an express contractual commitment to provide full-blooded 24x7 service should be able to do so—and customers should have a right of action if the service nonetheless fails to perform as promised.

Each of the criticisms set out above arises from the same fundamental problem. CAs are in a business that has a number of characteristics differentiating it from the more ordinary sales and licenses that appear to have been contemplated by the drafters of Article 2B. Rules designed for software licenses, access to LEXIS or Westlaw, or to marketing databases, simply do not work well when applied to a CA's provision of certificates and CRL lists. The difficulty of fitting an erratically shaped peg with substantially unknown tensile properties into even a good-sized round hole suggests rather strongly that Article 2B's attempt to draft comprehensive rules for e-commerce as an adjunct to its licensing rules was simply too ambitious.

D. Consumer Law and Electronic Transactions

Although section 2B-105(d) sets out a general principle that Article 2B will defer to a law that "establishes a consumer protection," this general principle is subject to four significant exceptions which substantially alter consumer protections for electronic transactions. The Reporter's Notes claims that these four derogations from state consumer law "reflect a limited approach that balances the modernization theme and the desire not to alter existing protection."[78] In so doing, however, Article 2B undermines the consumer law requirements it seeks to modernize and risks leaving consumers particularly vulnerable to more modern threats caused by hacked software and rogue electronic agents.[79] In this regard, it may be relevant to note that the UNCITRAL model law, which appears to have inspired at least some of Article 2B's approach to electronic contracting,[80] specifically defers to all relevant consumer law.[81]

Taken either individually or as a group, these four derogations are significant. First, any requirement that a contractual obligation, waiver, notice

78. *Id.* § 2B-105(d), Reporter's Note 6.

79. *See infra* text accompanying notes 105-116.

80. *See, e.g.*, U.C.C. § 2B-116, Reporter's Note 2 (Aug. 1, 1998 Draft).

81. *See UNCITRAL Model Law*, *supra* note 20, at art. 1, n.** ("This Law does not override any rule of law intended for the protection of consumers.").

or disclaimer be in writing is satisfied by "a record,"[82] which is defined as "information inscribed on a tangible medium or stored in an electronic or other medium and retrievable in perceivable form."[83] Thus, notwithstanding any state consumer law to the contrary, contractual terms, waivers, notices and disclaimers need not *actually* be retrieved by the consumer "in perceivable form"; the consumer need not even decline an offer to read it. The principle that an electronic message should have no less binding legal consequences and effects than one on paper seems entirely sensible and is a common theme in even the most modest law reform efforts relating to e-commerce. That modest and uncontroversial end is achieved by section 2B-113,[84] and by section 301 of the Draft Uniform Electronic Transactions Act (UETA).[85] But Article 2B's exception to the writing requirement in section 2B-104 goes farther than the minimum, since it does not require actual perception of the writing by either a human being or her electronic agents. For example, a sufficiently prominent link to a web site that contains required disclosures satisfies a disclosure requirement even if the consumer did not click on the link. Some consumer contracts today purport to incorporate by reference standardized terms that the ordinary consumer never sees; to the extent that online contracting puts those terms a click away, meaningful disclosure will be improved. But to the extent that state statutes require that contractual obligations, waivers, notices or disclaimers actually be visible to the consumer, enforcing clickwrap[86] contracts in which key terms are one hyperlink (or more?) away from the viewer does not further the objective of meaningful disclosure.

Second, a requirement that a contractual term be "signed" is satisfied by an "authentication."[87] Section 2B-102(a)(3)defines the act of authentication as:

> to sign, or otherwise to execute or adopt a symbol or sound, or encrypt or similarly process a record in whole or part, with intent of the authenticating person to:

---

82. U.C.C. § 2B-105(e)(1) (Aug. 1, 1998 Draft).

83. *Id.* § 2B-102(a)(39).

84. *See id.* § 2B-113 ("A record or authentication may not be denied legal effect, solely on the ground that it is in electronic form.").

85. UNIFORM ELECTRONIC TRANSACTIONS ACT § 301 (Sept. 18, 1998 Draft), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/eta1098.htm>.

86. Clickwrap licenses are "textual windows of non-negotiable, take-it-or-leave-it contract terms that prompt a user to 'click' assent [on a web form or program button] before allowing installation of a program or access to a website." Keith Aoki, *The Stakes of Intellectual Property Law* (visited Nov. 22, 1998) <http://www.law.uoregon.edu/~kaoki/AOKI.html>.

87. U.C.C. § 2B-105(e)(2) (Aug. 1, 1998 Draft).

> (A) identify the person;
>
> (B) adopt or accept the terms or a particular term of a record that includes or is logically associated or linked with the authentication or to which a record containing the authentication refers; or
>
> (C) establish the integrity of the information in a record which includes or is logically associated or linked with the authentication or to which a record containing the authentication refers.[88]

Under this definition, any application of a digital signature by a consumer to a contractual term proffered by a merchant, even one merely intended to attest to its integrity, theoretically could be considered a signature in the teeth of contrary consumer law. It would be unreasonable to intend that *any* type of authentication should satisfy a statutory requirement that a contract be signed, as opposed to those authentications that are intended to manifest an intent to be bound or which are commonly understood to manifest an intention to be bound. Alas, if one takes seriously the broad definition of authentication, other actions, which neither result from an intent to be bound nor manifest that intent, could be held to have contractually binding effects.[89] This is surely not what the drafters of Article 2B intend; rather, it seems to be an accident caused by the drafting style. Indeed, participants in the Article 2B drafting process insist vociferously that Article 2B adopts an intentionality requirement throughout and that no court would be so foolish as find that an authentication intended to serve only to show the integrity of a record had unintentionally served to form a contract.[90] The trouble is that section 2B-111 says clearly that a manifestation of assent is accomplished by an "authentication." And, despite what

---

88. *Id.* § 2B-102(a)(3).

89. *Cf.* U.C.C. § 2B-119(c) ("*Unless the circumstances indicate otherwise*, authentication is deemed to have been done with the intent to establish the person's identity, its adoption or acceptance of the record or term, its acceptance of the contract, *and* the integrity of the records or terms as of the time of the authentication.") (emphasis added).

90. *See, e.g.*, Letter from Donald A. Cohn & Mary Jo Howard Divley to Carlyle C. Ring (Oct. 12, 1998) <http://www.2Bguide.com/docs/cdm1098.html> ("What does it take for me to manifest assent to a license under the proposed draft? First, I must be acting either with knowledge or after having had an opportunity to review the record or term. (Under Section 112, if I don't have the opportunity to see the record before I pay for the product, I must be given the unconditional right to return it if, after I do see the record, I don't accept any part of it, even if the product is fine.) If I use conduct, I must intend that conduct and I must know or have reason to know that the other party may infer from my conduct that I assented to the record or term. ... Just because we are dealing with certain new subject matter does not mean that all courts will suddenly lose their reason.")

the drafters say they intend, an authentication can be any one of the things defined in section 2B-102, including authentications intended only to attest to message integrity. If one is going to enact a forward-looking reform of e-commerce law, it ought not to offer judges an opportunity to fall into easy formalist traps.

As a result of this possible confusion, in jurisdictions where Article 2B controls, well-advised parties will have to include disclaimers every time they use a digital signature, warning counter parties that "the use of this digital signature is not intended to create a contract." This is unhelpful and threatens to put a large damper on the growth of digital signature-based e-commerce.

Third, a consumer law requirement of assent to a specific contractual term is satisfied by "an action that manifests assent to a term in accordance with this article."[91] As of this writing, however, the section on manifestation of assent appears to be in a state of flux.[92] Currently, Article 2B provides several means by which assent may occur, including an authentication after an opportunity to review,[93] whether or not the review actually happened. Moreover, electronic agents can assent on behalf of their masters. The opportunity to review can be satisfied if it suffices to "enable a reasonably configured electronic agent to react to the record or term."[94] What a reasonably configured electronic agent might look like, however, nobody knows.

---

91. U.C.C. § 2B-105(e)(4) (Aug. 1, 1998 Draft).

92. For example, section 2B-111 of the August 1998 draft is heavily annotated with editorial cautions that the text has yet to be reviewed by the Drafting Committee. Similarly, the current UETA draft has bracketed section 107 on manifestation of assent, although it is clear that UETA intends to draw a sharp distinction between authentications and contractual commitments. *See* UNIFORM ELECTRONIC TRANSACTIONS ACT § 107 (Sept. 18, 1998 Draft), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/eta1098.htm> and accompanying notes.

93. Opportunity to review is defined in section 2B-112. The critical part of the definition reads:

> (a) A person or electronic agent has an opportunity to review a record or term only if the record or term is made available in a manner that:
>
> (1) in the case of a person, ought to call it to the attention of a reasonable person and permit review; or
>
> (2) in the case of an electronic agent, would enable a reasonably configured electronic agent to react to the record or term.

U.C.C. § 2B-112 (Aug. 1, 1998 Draft).

The Draft UETA section 108 contains similar language, but the section is bracketed for further discussion. *See* UNIFORM ELECTRONIC TRANSACTIONS ACT § 108 (Sept. 18, 1998 Draft), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/eta1098.htm>.

94. U.C.C. § 2B-112(a) (Aug. 1, 1998 Draft).

Last, but not least, a requirement in state consumer law "that a contractual term be conspicuous or the like" is satisfied by a term that meets the conspicuousness requirements of Article 2B. Currently, a term is "conspicuous" under Article 2B when it is:

> so written, displayed, or otherwise presented that a reasonable person against which it is to operate ought to have noticed or become aware of it. In the case of an electronic record intended to evoke a response by an electronic agent, a term is conspicuous if it is presented in a form that would enable a reasonably configured electronic agent to take it into account or react without review of the record by an individual. Conspicuous terms include but are not limited to the following:
>
> (A) with respect to a person:
>
> (i) a heading in capitals in larger or other contrasting type or color than the surrounding text;
>
> (ii) language in a record or display in larger or other contrasting type or color than other language or set off from other language by symbols or other marks that call attention to the language; or
>
> (iii) a term prominently referenced in an electronic record or display which is readily accessible and reviewable from the record or display; and
>
> (B) with respect to a person or an electronic agent, a term or a reference to a term that is so placed in a record or display that the person or electronic agent cannot proceed without taking some additional action with respect to the term.[95]

Thus, conspicuousness is explicitly satisfied by most conceivable types of clickwrap, or by a hypertext link to a page containing the required term even if the consumer does not visit the page and is thus not actually exposed to required language, so long as "a reasonable person ... ought to have noticed or become aware of it."[96] Current browser and e-mail technology makes it difficult, albeit not impossible, for the author of an electronic document to control how the reader will display it. It follows that familiar paper-based requirements such as a minimum sized typeface probably should not be carried over to electronic contracts. Reliance on prominence and the reasonable reader may well be the best one can do, but it will nonetheless invite dispute and litigation.[97]

---

95. *Id.* § 2B-102(a)(9).

96. *Id.* § 2B-102(a)(9).

97. Reporter's Note 4 to section 2B-110 ("Bizarre and oppressive terms") states that "[u]nconscionability doctrine allows courts to monitor and limit application of [common

Taken as a group, these four provisions constitute a significant weakening of consumer protections in the electronic world. The Reporter's Note is disingenuous when it claims that "[t]he limited approach adopted here contrasts to non-uniform digital signature statutes enacted in several states which replace or amend all signature and writing requirements, including consumer statutes."[98] In fact, there appear to be no state digital signature statutes which have any effect on consumer protection rules, other than allowing an electronic record to substitute for a paper signature.[99] It is technically true that the approach in Article 2B contrasts to the prior practice of leaving consumer protection rules equally applicable to e-commerce. The approach in Article 2B may or may not be correct, but it is certainly not limited, and the difference is that Article 2B alters consumer protections to the consumers' likely detriment.

Meanwhile, whether a CA gives an implied warranty of accuracy for its CRL turns on whether the contents of the CRL are "published informational content" or mere "informational content." Article 2B defines "published informational content" as "informational content prepared for or made available to recipients generally or a class of recipients in substantially the same form and not customized for a particular recipient by an individual that is a licensor, or by an individual or group of individuals acting on behalf of the licensor, using judgment or expertise."[100] A CRL fits that definition fairly well. However, the definition goes on to exclude

---

law principles] in a way that avoids binding the assenting party to unknown terms that are bizarre and unfairly oppressive." *Id.* § 2B-110, Reporter's Note 4. This seems to suggest that unconscionability might be invoked to correct gross defects in the process of contract formation, as well to correct grossly unfair contract terms, if electronic agents run wild. I find this to be a very intriguing idea—but one that is absent from the text of section 2B-110.

98. *Id.* § 2B-105, Reporter's Note 6. No examples are offered—probably because there are none. *See infra* note 99.

99. Other than stating the circumstances in which an electronic message may satisfy a writing requirement, most of the state digital signature statutes to date, including the influential Illinois statute, are silent on the subject of consumer protection. When they do address the issue, they add, not subtract, protections for consumers. For example, the Washington Electronic Authentication Act makes it clear that while agreements between a CA and a subscriber may vary many of the provisions of the Authentication Act itself, "Nothing in this chapter shall be construed to eliminate, modify, or condition any other requirements for a contract to be valid, enforceable, and effective." WASH. REV. CODE § 19.34.320(2)(b) (1997). Additional consumer protections include forbidding a CA from disclaiming or limiting warranties that a certificate has no known false information, and that the certificate satisfies all material requirements of the statute. A CA is also required to give a warranty that it has not exceeded limits of its license (e.g., the reliance limits). *Id.* § 19.34.220(1).

100. U.C.C. § 2B-102(a)(36) (Aug. 1, 1998 Draft).

"informational content provided in a special relationship of reliance between the provider and the recipient."[101] It seems reasonable to say that a CA has just such a special relationship with anyone who relies on its CRL. The problem is that, in some models, anyone in the world may be able to access the CRL and may have a need to do so. It is one thing to say that the CA has a special relationship with its clients; without more guidance, courts may be reluctant to impose a heightened duty on a CA that potentially runs to the whole world.[102] The distinction is potentially significant because under section 2B-404, there is no implied warranty of accuracy for published information content,[103] but there is such a warranty when a special relationship of reliance exists. On the other hand, even if a CRL is not published informational content, Article 2B allows a CA to disclaim all warranties of accuracy for its CRL unless there is something in state digital signature law to the contrary, or a court would find it unconscionable.[104]

The potential impact of Article 2B, and the possible harm to the unlucky or unwary, becomes much greater when one considers the ways in which Article 2B treats automated commerce. Article 2B contemplates "automated transactions," defined as "contract[s] formed by electronic means or electronic messages in which the actions or messages of one or both parties will not be reviewed by an individual in the ordinary course."[105] As a person is usually considered to intend and be responsible for the ordinary and foreseeable results of her actions, codification of a rule generally making people responsible for the acts of their electronic agents[106] changes little of substance, while usefully removing any doubts that might exist about the validity of agent-based commerce. It does not necessarily follow, however, that agent-based commerce is appropriate for all types of transactions. In particular, given how little is known about how agent-based commerce might work at the consumer level, if a state consumer law rule requires conspicuousness, one might reasonably expect that a uniform rule would say that those transactions cannot be consummated without first actually securing some manifestation of approval by the electronic agent's human principal. Instead, Article 2B removes any

---

101. *Id.*

102. *See* Froomkin, *supra* note 9.

103. *See* U.C.C. § 2B-404(b)(2) (Aug. 1, 1998 Draft).

104. *See id.* §§ 2B-404 to 2B-406.

105. *Id.* § 2B-102(a)(4).

106. "'Electronic agent' means a computer program or other automated means used by a person to independently initiate or respond to electronic messages or performances on behalf of that person without review by an individual." *Id.* § 2B-102(a)(19).

need for human intervention, stating that a term is conspicuous "if it is presented in a form that would enable a reasonably configured electronic agent to take it into account or react *without* review of the record by an individual."[107] Article 2B is more solicitous about the limited capacities of agents than of people: if a person has reason to know he is dealing with an electronic agent and proffers a contract term "to which the electronic agent could not react" *regardless of whether the person proffering the term knew or could have known of the agent's limitations and regardless of whether the agent was "reasonably configured,"* then the term is not part of any otherwise binding contract formed between the person and the agent.[108] People with limited capacities to wade through contractual terms do not get an equivalent solicitude.

In a world in which (Article 2B notwithstanding) some companies may increasingly be releasing the source code of their programs into the public domain so as to encourage third-party volunteer improvements,[109] the danger of hacked copies of desirable programs will become more and more significant. If some of these programs (e.g., web browsers enabled for commerce) are hacked in a way that causes agents to ignore warnings about critical terms or to engage in other rogue behavior undetectable by the average user until well after the fact, the consequences for unlucky consumers might be quite severe, especially if "[o]perations of an electronic agent constitute the authentication, manifestation of assent, or performance of a person if the person used the electronic agent for such purpose."[110] If Bob acquires and uses an e-commerce enabled web browser that unbeknownst to him has been hacked to order gifts for random strangers and arrange direct e-mailed or shipping, did Bob use the rogue electronic agent "for the purpose" of making transactions? Yes. For the purpose of making *those* transactions? No, since the transactions were not intended. But under Article 2B, and perhaps under pre-Article 2B law as well,[111] Bob may be liable anyway.

---

107. *Id.* § 2B-102(a)(9) (emphasis added).

108. *See id.* § 2B-204(3) ("The terms of a contract formed under paragraph (2) are determined under Section 2B-207 or 2B-208 [relating to mass-market contracts], as applicable, but do not include terms provided by the individual in a manner to which the electronic agent could not react.").

109. *Cf.* Paul Phillips, *Why Mozilla Matters* (visited Nov. 9, 1998) <http://www.mozilla.org/why-mozilla-matters.html>.

110. U.C.C. § 2B-119(a) (Aug. 1, 1998 Draft).

111. *See also id.* § 2B-110, Reporter's Note 4:

> In some cases, however, automation may produce unexpected results because of errors in program, problems in communication, technological 'bugs', or other unforeseen circumstances. When this occurs,

According to section 2B-116, "an electronic authentication, message, record, or performance is attributed to a person if ... (2) the receiving person, in accordance with a commercially reasonable attribution procedure for identifying a person, reasonably concluded that it was the action of the other person or the person's electronic agent."[112] In other words, if the merchant correctly authenticated Bob's digital signature, as supplied by the rogue agent, then in the absence of contrary agreement or regulations, this "creates a presumption that the authentication, message, record or performance" was Bob's. Even if Bob figures out what is going on, and successfully rebuts the presumption that he wanted to send flowers to every member of Congress, Bob is "nevertheless liable for losses of the other party in the nature of reliance if the losses occur" if he failed to exercise reasonable care.[113] It would be churlish to complain that the drafters do not give any hint of what reasonable care might be since it is fairly clear that no one currently has any idea.

Article 2B contemplates that e-commerce may go wrong and provides a section, section 2B-118, that deals with "electronic error." This section defines electronic error as "an error created by an information processing system, by electronic transmission, or by a consumer using an electronic system, if a means for correction or avoidance of such errors was not reasonably provided." But section 2B-118 is oddly quiet on who should have reasonably provided a means of error-correction. Suppose Bob's hacked browser orders 1,000 copies of Tetris when Bob is sleeping. Who has the

---

> common law concepts of mistake apply, as do the provisions of Section 2B-118 ["electronic error"—see *infra* note 114 and accompanying text]. In addition, unconscionability doctrine may be used to prevent oppressive results caused by the breakdown in the contracting process. While automated transactions are a new setting for this doctrine, the safeguards it supplies are important for this type of commerce.

Id. § 2B-110.

112. *Id.* § 2B-116(a).

113. *Id.* § 2B-116(c). Other requirements, satisfied in the hypothetical in the text, are that:

> (2) the other party reasonably relied on the belief that the person was the source of an electronic authentication, message, record, or performance,
> (3) the reliance resulted from acts of a third person that obtained access numbers, codes, computer programs, or the like from a source under the control of the person rebutting the presumption; and
> (4) the use of the access numbers, codes, computer programs, or the like created the appearance that it came from the person rebutting the presumption.

Id. § 2B-116(c).

burden of providing the means of correcting the error? Bob? The merchant with whom Bob's malicious intelligent agent transacts? Or the original manufacturer of Bob's browser? The Reporter's Note suggests that in this hypothetical the merchant has the duty to send Bob a confirmatory e-mail,[114] which sounds like a good start, although it would be more reassuring if the text of section 2B-118 spelled that out clearly. In the absence of electronic error—i.e. in the presence of the reasonable provision for correction of error such as the confirmatory e-mail—Bob has no recourse under section 2B-118. Thus in the example above the merchant can demand that Bob pay for the 1000 copies of Tetris even if Bob never read the e-mail, or had reason to expect that he should be checking his e-mail, and the copies were delivered to a third party without his knowledge.[115]

Even if there is the right sort of electronic error Bob escapes liability under section 2B-118 only in very limited circumstances:

> (b) In an automated transaction consumer transaction, the consumer is not bound by an electronic message that the consumer did not intend and which was caused by an electronic error if the consumer:
>
> (1) promptly on the earlier of learning either of the error or of the other party's reliance on the message:

---

114. The Reporter's Note to section 2B-118 offers two illustrations:

> *Illustration 1:* Consumer intends to order ten copies of a video game from Jones. In fact, the information processing system records 110. The electronic agent maintaining Jones' site disburses 110 copies. The next morning, Consumer notices the mistake. He sends an E-Mail to Jones describing the problem, offering to immediately return or destroy copies; he does not use the games. Under this section, performing on these offers means that there is no presumption that the contract was for 110 copies. If it desires to enforce the apparent contract, Jones must prove that there was no error.
>
> *Illustration 2:* Same facts, except that Jones' system before shipping sends a confirmation, asking Consumer to confirm that it ordered 110 games. Consumer confirms 110 copies. This section no longer applies. If Consumer sees the confirmation request and does not respond, the section also does not apply. In either case, the system reasonably allowed for correction of the error.

Id. § 2B-118, Reporter's Note.

115. *See id.* § 2B-120 ("an electronic message is effective when received even if no individual is aware of its receipt. If an offer in an electronic message initiated by a person or an electronic agent evokes an electronic message in response, a contract is formed: (1) when an acceptance is received ...").

> (A) in good faith notifies the other party of the electronic error and that the consumer did not intend the original message; and
>
> (B) delivers all copies of any information it receives to the other party or delivers or destroys all copies pursuant to any reasonable instructions received from the other party; and
>
> (2) has not used or received a benefit from the information or informational rights or caused the information or benefit to be made available to a third party.[116]

These conditions resemble what a court might reasonably conclude under common law principles in a case with only two parties involved. But what if Bob's rogue software was configured to forward the Tetris software to one or more third parties without ever troubling Bob about the matter? Perhaps section 2B-118(b)(2) could be modified to require that Bob intentionally or knowingly have made the benefit available to another?

E. Liability Rules

The issue of liability rules and presumptions is perhaps the most controversial aspect of digital signature laws.[117] When digital signature laws exist and speak to the question, they will trump the relevant portions of Article 2B, although the interaction of Article 2B's choice of law principles and state digital signature laws may create some confusion. When a state does not have a digital signature statute, or has a statute that does not address liability issues, Article 2B's provisions will control.

Article 2B sets up a liability regime by which a person who uses a secure electronic authentication procedure, such as a digital signature, and then negligently loses control of that digital signature, is liable for all losses in the nature of reliance in transactions to which Article 2B applies that are caused by that negligence. If Bob, not fully understanding the implications or use of new technology, allows Alice to obtain access to Bob's computer, other device, PIN, or passphrase that will allow Alice to use Bob's digital signature, then, according to section 2B-116, Bob is responsible for paying the reliance costs caused by Alice's subsequent spending

---

116. *Id.* § 2B-118.

117. For a summary of the issues see C. Bradford Biddle, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, 33 SAN DIEGO L. REV. 1143 (1996).

spree.[118] Bob's proof that it was really Alice is of no use if the merchant reasonably relied at the time of sale, and in most cases it will be reasonable to rely on a digital signature backed by a valid certificate. As there is no equivalent to a credit limit in digital signature-based commerce, the liabilities that Alice could impose on Bob in seconds, perhaps with the aid of an electronic agent or two, is theoretically unlimited.

"Non-repudiation," that is, Bob's inability to escape from having to compensate parties who reasonably relied on Alice's claim that she was Bob, is one of the top items on the legislative agenda of those who hope to have digitally signed electronic purchasing replace credit and debit card transactions. Armed with a guarantee of non-repudiation, CAs should be able offer a transaction mechanism with much lower overheads than credit cards since the trusted third party would no longer function as a sort of insurer of the validity of the transaction—the law would. Non-repudiation contrasts dramatically with consumer habits and expectations engendered by credit cards, although the customer's ability to unwind transactions that use debit cards depends more on bank practices than law.[119]

Most states that have considered the issue have rejected the strong form of non-repudiation included in Article 2B. The specter of "grandma losing her house because she lost control of her digital signature" has simply proved too frightening.[120] Rejected proposals leave their traces, if any, in legislative history, not the statute books. Thus, although many states concluded that they did not wish to enact non-repudiation rules placing most or all potential liabilities on parties other than CAs, the nature of the legislative process ensures that these decisions to reject or defer the issue are not memorialized in law. It follows that were Article 2B's liability rules to be enacted, they would take effect even all states that do not have explicit contrary rules in their digital signature laws, even if they considered and rejected the idea.[121]

There are some sound policy arguments in favor of non-repudiation in e-commerce, such as when the transacting parties are both sophisticated, or the electronic transactions are sufficiently unusual that all parties under-

---

118. Recall that, under U.C.C. § 2B-116, " an electronic authentication, message, record, or performance is attributed to a person if ... (2) the receiving person, in accordance with a commercially reasonable attribution procedure for identifying a person, reasonably concluded that it was the action of the other person."

119. *See* 15 U.S.C. § 1643(a)(1)(B); 12 C.F.R. § 205.6 (1995) (limiting liability to $ 50 for most unauthorized electronic funds transfers).

120. For what it's worth, I believe I originated this now-widespread meme in 1995, in my participation on the ABA Digital Signature Guidelines drafting process.

121. Recall that section 2B-105(g) grandfathers digital signature statutes.

stand that the technology is not used casually. My personal view happens to be that the case for non-repudiation of digital signature-based consumer transactions remains to be proved. Whether I am correct about that or not, a very significant amount of public debate and consumer education would be required before imposing potentially unlimited ability on the Bob's of the world, or on parents or grandparents of any gender. Perhaps that case could be made. It has not been made in Article 2B, and a statute about the rules appropriate for licenses relating to ever-shrinking types of intellectual property[122] is an inappropriate vehicle for such sweeping changes in electronic transactions law generally. Article 2B's adoption of strong non-repudiation contrasts with the revised draft UETA. Where once UETA included presumptions that Bob would have had to rebut, now the draft is neutral on the entire question of the legal effect of a reliance on a digital signature.[123]

III. CONCLUSION

The Reporter's comment that "Article 2B will have little impact on established commercial practice" because "[e]ven with a broad scope ... most provisions can be altered by agreement and defer to customs of trade, course of dealing, or formal contracts"[124] seems somewhat optimistic when applied to e-commerce, since so often there are no customs or usages of trade to fall back on.

---

122. The Recording Industry Association of America, the National Association of Broadcasters, the National Cable Television Association, the Newspaper Association of America, the Magazine Publishers of America, and the Motion Picture Association of America have each expressed opposition to Article 2B or asked that their industry be excluded from it. *See, e.g.*, Letter from Cary H. Sherman, Senior Executive Vice President and General Counsel, Recording Industry Association of America to National Conference of Commissioners on Uniform State Laws (Oct. 9, 1998) (expressing opposition and noting similar views of other trade associations), *available at* <http://www.2Bguide.com/docs/riaa1098.html>. *See also infra* note 128 (noting suggestion by Director of ALI and other influential lawyers that scope of Article 2B should be limited).

123. The current draft's language is in flux, but reads "[a]n electronic record is attributable to a person if ... [an] other person, in good faith and acting in compliance conformity with a commercially reasonable security procedure for identifying the person to which the electronic record is sought to be attributed, reasonably concluded that it was the act of the other person, a person authorized by it, or the person's electronic agent." UNIFORM ELECTRONIC TRANSACTIONS ACT § 202 (Sept. 18, 1998 Draft), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/eta1098.htm>.Even when a record created by Alice is "attributable" to Bob, it has only "the effect provided for by the agreement regarding the security procedure." *Id.*

124. U.C.C. § 2B-104, Reporter's Note 1 (Aug. 1, 1998 Draft).

For a legislature to pass Article 2B in its current form would be akin to installing a beta version of a large and complex operating system. Modern operating systems and software suites often attempt to occupy the field and provide an array of extensive, complex, and often poorly documented or understood features.[125] Some parts of the package may have strange interactions with software already installed on the system while other parts may assume the existence of hardware or software that is still in development (e.g., the reasonably configured electronic agent). Article 2B's enormously ambitious strategy of providing a full regime for the sale and delivery of licenses in information resembles one of these self-installing software suites. While some of the rules regarding electronic contracting may be defensible, or even sensible, the total package makes a series of policy choices, especially those displacing consumer law for online transactions and enacting a national law on non-repudiation for digital signature-based e-commerce which do not seem to be required to achieve the end of rationalizing the law of information licenses.

As an abstract proposition, Article 2B represents a praiseworthy attempt to identify problems and solve them early. It is surely correct that "[t]ypically, U.S. law is drafted in retrospect. Years of informal standards are developed and then codified. Article 2B is an attempt to get ahead of that curve."[126] There is a strong case to be made for writing uniform laws that will achieve the "optimal impact for the modernization themes developed with reference to electronic commerce." That case does not appear very clearly from Article 2B, nor does it appear that Article 2B's vision of what optimization looks like is necessarily the one that legislatures and the public would or should share. Whether or not Article 2B embodies the best vision of online contracting rules, it seems distinctly sub-optimal to adopt a special set of online contracting rules that would apply only to licenses in information (whether or not part of a larger sale), or only to mixed transactions in which the information license component was sufficiently great. Today at least, the look and feel of online shopping is much the same whether the thing being purchased is a CD-Rom with a program on it, a book, or computer part. If uniform laws are to be written for e-commerce, they should cover all of it, not perpetuate the patchwork we already have by overwriting new cleavages onto an already fractured law.

---

125. *See* Yannis Bakos & Erik Brynjolfsson, *Aggregation and Disaggragation of Information Goods: Implications of Bundling, Site Licensing and Micropayment* (visited Oct. 24, 1998) <http://www.stern.nyu.edu/~bakos/aig.pdf>.

126. Letter from Terrence Maher, to Editor, *San Francisco Chronicle*, (June 17, 1998), *available at* <http://www.2Bguide.com/docs/tmaherrre.html> (visited Nov. 23, 1998).

And when those uniform rules are written, they must take due account of consumer law's considered mix of paternalistic rules and the correction of market failures created by information asymmetries, as well as taking account of consumer expectations and usages of trade.

Here, Article 2B says it well:

> [Quoting Grant Gilmore:]
>
> > The principal objects of draftsmen of general commercial legislation ... are to be accurate and not to be original. Their intention is to assure that if a given transaction ... is initiated, it shall have a specified result; they attempt to state as a matter of law the conclusion which the business community apart from statute ... gives to the transaction in any case. But achievement of those modest goals is a task of considerable difficulty.
>
> To be accurate and not original refers to commercial practice as an appropriate standard for gauging appropriate contract law unless a clear countervailing policy indicates to the contrary or the contractual arrangement threatens injury to third-party interests which social policy desires to protect. Uniform contract laws do not regulate practice. They sustain and facilitate it. The benefits of codification lie in defining principles consistent with commercial practice which can be relied on and are readily discernible and understandable to commercial parties.[127]

Despite some improvements in the most recent drafts, as regards its e-commerce rules Article 2B does not meet the high standard it rightly sets for itself.[128]

---

127. U.C.C. Art. 2B, Default Rules (quoting Grant Gilmore, *On the Difficulties of Codifying Commercial Law*, 57 YALE L. J. 1341 (1957)).

128. On October 7, the Director of the ALI joined in a letter requesting substantial changes to Article 2B, including narrowing the scope to apply only to information subject to "informational right" as defined in section 102(a)(27) and the removal of all sections relating to contract formation by electronic means. *See* Memorandum from Geoffrey C. Hazard, Jr. et al. on July 1998 Draft Suggested Changes to Article 2B Drafting Committee (Oct. 7, 1998) *available at* <http://www.2Bguide.com/docs/gch1098.pdf> (visited Nov. 23, 1998). This is a very encouraging development.