Federal Case Indicates the Need for Information Age Reforms in Business, Policy and Law

By Daniel Greenwood*

November 17, 1997

Judge Porfilio of the Tenth Circuit (No. 96-1462, 9/30/97 and available at www.tiac.net/biz/danielg) recently held that a computer record did not constitute a "writing" under the Bankruptcy Code. The case, In re Kaspar, deals with a lender that tried to avoid having its loan discharged in bankruptcy by claiming that the debtors' statement of financial condition was materially false. However, the Bankruptcy Code provides an exception from discharge only if the materially false statement on which the lender relied was in writing. In this case, the information was obtained from the debtors over the telephone and entered into a computerized form by the lenders' representative, who then read the information back to the debtors to verify it had been entered correctly. The court held that this did not constitute a writing, concluding with this invitation to Congress:

"We note with some wryness that in this instance the law lags behind technology and custom, but that gap is a subject which must be addressed to the Congress and not the courts. We will not undertake to rewrite the express language of a statute merely to accommodate the commercial conveniences attributable to modern technology."

The Kaspar case is important both for what it requests and what it rejects. The judge makes a very good plea for Congressional reform of writing and signing requirements that exist in federal statute. However, the judge refuses to use the power of the judiciary in this case to interpret these requirements to be consistent with modern practices and electronic media. It is instructive that the judge noted, as a policy basis of his holding, that exceptions to discharge under the bankruptcy statute are interpreted narrowly.

In view of this type of admirable judicial restraint, the current Massachusetts Electronic Records and Signature Act specifically includes guidance to the judiciary in the following terms:

> **Section 5. Writings and Signatures Generally.**
> ". . . In general, where any rule of law purports to specify a particular medium for the creation, storage, communication, or authentication of any records or information, that requirement shall be liberally construed to allow the broadest possible use of electronic or digital methods unless there is clear public interest to the contrary."

In the Kaspar case, had federal policy makers enacted a statute like the proposed Massachusetts Act, then the judge who is so concerned with following statutes to the letter would have been encouraged to interpret the writing requirement more broadly. In cases where no particular public interest compels narrow interpretation of a writing or signature requirement, then this statutory provision should permit and even direct the judiciary to allow a record consisting on any medium to meet the writing requirement. The judge would have had more latitude to hold that the debt incurred based on a false statement of financial condition would not be discharged - irrespective of the media used to transmit, record or create the record.

As more transactions take place electronically, including transaction that will require some solemnity, the question should be: how shall we express enfeoffment electronically? Enfeoffment was the act of going to the land and handing over a twig ceremonially in front of witnesses to signify the purchase and sale of land. This act was done to solemnify the transaction. The policy behind this somemnification was, in part, to assure there was no mistake about the nature and gravity of the transaction. How should such solemnity be achieved via communication technologies that allow for remote parties to transact business?

When some people indicate that this is a security issue I feel that is like saying: building a house is a hammer and nails issue. In the first place, we have an architectural question: what design requirements exist to create a structure that serves the purpose and won't fall down when pushed? Then we use the available tools to construct it. In this case, we construct an interface, application, network and records management environment that is replete with appropriate practices and agreements). What are the minimum requirements of this environment? There will almost certainly be a need for security dimensions as well. However, here, the mere "signature" and "writing" requirements are not met by secure systems but by understandable systems. Why should synchronous phone interactions by the parties buttressed by contemporaneous entries into a database be inadequate?

I believe that the judge failed to adequately weigh the fact that the electronic record in question was comprised of verified answers to credit data supplied by the Kaspars themselves and entered into a computer and database by a loan officer based on contemporaneous transcription. According to the opinion: "the loan representative then read the figures back to the Kaspars who orally verified their accuracy" and it was based on this exchange that the electronic record was authenticated and relied on by the lender. As usual in cases involving the validity of electronic records and authentication, the issue litigated in this case did not involve attempted repudiation or the integrity of the data. The Kaspars apparently did not contest the integrity of the electronic record or that they had in fact assented to the information for the purpose of creating a complete loan application with terms and conditions binding each party.

The facts of the case require more detailed analysis. What if the Kaspars had used a personal secretary to type their application for them? Imagine that they simply dictated the information to their secretary who faithfully and accurately input the data and who then signed and delivered the application at the Kaspar's behest and on their behalf. Does this become a stronger case if the secretary reads back the information to the Kaspar's to verify the accuracy? I assume no writing formality issue would arise under those facts and that the debt would not have been discharged. What if a computer were used by the Kaspar's agent? Obviously, it no longer matters as a matter of law that computers are used to generate records that are printed on paper and then delivered. But what if the electronically signed computer record were delivered to the loan officer in electronic form - say on disk or by e-mail? Why should that make any difference to the legal result?

The fact that the Kaspars never actually "saw . . . the application form entered into the computer" made an impression on the judge. This is especially interesting because today, if you ask a really good cognitive psychologist, she will tell you that some people comprehend spoken information far better than data presented to them on a form (I would expect this applies double to most financial forms I have seen). Unlike simply looking at a financial form on paper, the Kaspars enjoyed the rare cognitive benefit of having their information carefully read back to them so that they had the occasion to hear every bit of information submitted. Ears - unlike eyes, can not so easily close or turn their attention to another location. This information was not only tendered by the Kaspars only minutes before in response to direct question, but it was, in effect, then deposited by the loan officer directly back into the conscious minds of the applicants for their informed assent. The Kaspars could not help but know what they were assenting to and acknowledge the basis of the loan transaction they were undertaking. Furthermore, the judge can not seriously expect that seeing information is a prerequisite for creating a legally binding writing. Blind people would be at a bit of a disadvantage and so would a lot of dictators (in the amanuensis sense - not the Saddam Hussien sense).

I do not suggest that the holding was unsupportable - only that it points out the need for deeper thinking about the suitability of electronic records and authentication under the law. Nor do I fault the judge for coming to this holding. Perhaps the judge desired to make a point that law and policy makers need to reach consensus about exactly what practices will constitute enforceable and valid records and authentication. I could not agree more. Merely indicating by statute that all writings and signatures may be electronic is not good enough for many situation that require some clearer indication that a party understands and agrees.

The judge goes to great pains to point out that false statements of financial condition, to qualify under this exception, must be in written form due to the solemnity of the transaction. The court notes that:

> "giving a statement of financial condition is a solemn part of significant credit transactions; therefore, it is only natural that solemnity be sanctified by a document which the debtor either prepares or sees and adopts. In a world where important decisions relating to the extensions of credit and service will be made upon the contents of a statement relating to financial condition, too much mischief can be done by either party to the transaction were it otherwise. Somewhere in the commercial risk allocation picture, the writing must stand as a bulwark which tends to protect both sides. A creditor who forsakes that protection, abandoning caution and sound business practices in the name of convenience, may find itself without protection."

But, in a digital world, what is the meaning of the word "prepares?" When should a voice recognition systems that meets sufficient quality benchmarks be granted the status of a legitimate method of preparation? When is such a system to be considered part of a "sound business practice?" What is the meaning of "sees and adopts?" A return e-mail that confirms an application and is assented to would presumably qualify. The typical question asked at this point is "what evidence of adoption is necessary to prevent subsequent denial?" Click to adopt? Type your name in the "I _____ hereby adopt" space? Use your password? Must we use our cryptographic digital computer-steroid signature? While this question can be important, these cases are seldom about repudiation. Too much other business context typically exists to prevent such a shallow claim. Rather, the issue is one of setting clear technical and practical benchmarks so every party to such a transactions knows and can be shown to have known that they have acted to create a binding document. I do not believe that use of a particular technology is enough to achieve this. No matter how good a given digital signature system may be, for example, if the issue is not about repudiation and message integrity, then the system is not relevant.

What is needed here, among other things, are simple and widely understood methods to symbolize an agreement reached via an electronic network. For example, imagine an interface where the contract (or application, or weekly time sheets, etc.) appeared as an object. When you were ready to "sign" the object, you simply moved it into the zone on your screen (or into a special directory, or through a designated router, etc.) where you push the documents that legally bind you. Perhaps a warning message comes up asking if you in fact want to be bound? Perhaps the interface or application would not permit assent for a given "solemn" agreement to be complete until an oral voice annotation of assent were also associated with the object in addition to simple clicking. Or, (with the help of design-aware interface engineers) perhaps we settle on shapes that symbolize each stage of drafting and acceptance up to final binding assent. The object representing the first draft may look like a circle and the lines on opposite sides get closer together until you agree to a flat line that represents final agreement. A contract with one final provision to be hammered out could look like a flat line with one bump (of course, the bump is linked directly to the provision in question). Alternatively, sounds or even gestures could suffice (this is more far out technically, but the technical implementation is far less important than the policy goal).

The point is that we need widely accepted ways to represent the thresholds of legality afforded records in electronic form - especially records that are the subject of multi-user inputs and that have legal consequence. By multi-user, I mean records that go back and forth among drafters or negotiators or co-workers, etc. I don't really care what those symbols are (though they need to accommodate people

with various disabilities, including sight, hearing or tactile impediments) but they should be widely understood - just as a manual signature is today. The PenOp system (which allows people to manually sign electronic data) fulfills many of these policy goals. However more robust interface standards are needed to accommodate all technologies that would create legally binding agreements because we need systems that will create predictable outcomes. Assuming that more than one technology is available to prove assent was manifested, the screen or other interface metaphors should still remain as consistent as possible for the sake of end-user simplicity and the creation of reasonable expectations.

The best way to assure a predictable outcome is not to legislatively mandate "this is how you make an enforceable contract on the Internet" - but rather we should create an systems that people would want to use because they are efficient and desirable and that also meet the policy requirements for signaling unmistakably when a deal is sealed. In other words, the market should evolve the systems and practices. These systems are sorely needed to make networks truly useful for business. One may be electronically drafting a contract, submitting an application, or even making a parliamentary motion before a Board of Directors that is meeting in an online conference (synchronous or asynchronous). Every participant in that Board meeting (or Town Meeting, or Hearing, etc.) should be able to see what motion is "on the table" and see when an amendment has been accepted and changed the motion, etc.

Little naked encrypted message digests of hash function results bouncing around my computer - while technically potentially useful - are just are not good enough. Nor are biometrics by themselves or any other "security" system. In a sense, this can be seen as an electronic records management issue. This is also certainly an interface issue. There is a "security" component (to the extent one needs to link the records and authentication to a source for example). At core, however, this is a business standards issue. Just as there have emerged a multitude of business practices that are now reflected in the Uniform Commercial Code, so to must there develop general usages for electronic records and authentication. People need "simple to comprehend" symbols and methods to know where they stand - and the law should support rational and accepted practices that arise to meet this need.

The Kaspar judge noted that the loan practices were common in the industry. If the use of a phone for dictation and input into a database with final assent based on a "read-back" were to be the norm, and if that were widely accepted, then the law should support these practices. However, I suspect these particular practices, (while perhaps common in this particular financial market slice, for that purpose and at that time) will not be the widely used in electronic commerce because they are not "machinable". That is, the Kaspar scenario required a live human on the bank side who actually took down the information and read it back for approval. Frankly, I would be shocked if electronic commerce systems reached this level of effectiveness in the foreseeable future. Clearly, there will come a day when loan applications will be done entirely over networks (probably with the creditor's systems and not people). What systems and practices should the law recognize as valid for such purposes?

Some might argue that the main issue in the Kaspar case is that "the DEBTOR and not the lender must make the statement in writing?" The statute provides, in relevant part, that a debt shall not be discharged to the extent it was "obtained by use of a statement in writing that is materially false . . . that the debtor caused to be made or published with intent to deceive...." The statement undeniably originated from, is attributable to and was verified by the Kaspars. They "caused" the statement to be reduced to writing. In what sense did they fail to make the statement? Do their fingers need to be on the keyboard? Why?

The Graham case (cited in Kaspar) held that: "defendants caused a written statement regarding their financial condition to be published by providing plaintiff's telephone solicitor the financial information contained on the written application for a credit card. A written statement does not have to be physically prepared by a defendant. The requirements of 523(a)(2)(B) are met if the existence of a written statement was caused to be prepared by the defendant."

It sure looks to me like the existence of a written (electronic) statement was caused to be prepared by the Kaspars. It might also be argued that the Kaspar's never signed or authenticated the form. But why is voice authentication and assent inadequate? In any case, there is no direct "signing" requirement in the statute - just a writing requirement. The Kaspars are not attempting to repudiate the fact that they orally made these statements. Authentication and signing are, in a sense, moot points here.

I would assert that the case created an anomalous result. That is, the law was interpreted in a way to allow a couple of people to get out of paying debt that they incurred which would not have been discharged had it not been for a shallow technicality. Perhaps this was the correct legal interpretation - but the result is nevertheless puzzling. If the statement came from their computer and was printed and mailed then this would be a non-issue - I assume the debt would not have been discharged. Similarly, if they dictated it to their computer (using voice recognition software) without looking, it would still be a non-issue. If the computer were in another room in their house, perhaps using a voice recognition system connected by a local area network, then this would still be a non-issue I would wager. In each case, the record was originated by and caused to be made by the defendant. Is the rule that one may not opt against visually reviewing applications in favor of the same online audio media available to the blind? May only blind people create, review and approve valid electronic records in this manner? If this is the proposed rule, then how bad must one's eyesight become before she may avail herself of this potentially superior method of managing records and conducting business?

If the key issue is not that the application must be personally typed and visually reviewed, then why should it matter where the record is created? If the computer were in the home of a friendly neighbor of the defendant, connected by a wide area network, activated by a voice recognition system in the Kaspar's house, and then printed and mailed, would the result change? What if a party finds it convenient or cost-effective to house voice originated record creation systems in a data center shared by several businesses? The

parties use their phones from the efficient comfort of their office or home and get voice and/or text verification. Would only text verification be acceptable? What if a verification service were outsourced? In these cases, from the point of view of the lender, a paper record would be received which the defendant caused to be made. When the record is entered in a computer in the lender's office connected by a network ("voice protocol") to the defendant who originated the record and caused it to be made, why does the result change?

Why would this be different from the Kaspar case? The Kaspar's apparently did not argue that the lender had altered the record or that the record was inaccurate. Where is the line to be drawn? What systems, applications, network environments and practices shall create valid applications?

Whatever the law accepts, it is in the interests of general electronic commerce that the practices and systems be as consistent as possible across private economic sectors and the public sector. It would lead to confusion for too many different, perhaps contradictory, systems and practices to emerge. The simple example would be that banking agreements are final when you move the document to the right and leases are final when you move them to the left - hence creating defenses where none should exist. More realistically, sending an S/MIME message may mean "draft" in one circumstance and "final agreement" in another context. Some way must evolve for people to simply tell when they are doing something that is final and/or binding. In short, we need to evolve standards - not in the narrow technical sense (ANSI, NIST, etc.) but in the sense of widely accepted combinations of technology, business practice and legal treatment. Though the law should follow practice in this area because the market is so dynamic and young (it can be said to be in a state of mitosis) I think a good start would be abolishing explicit legal requirements for paper and ink.

The Kaspar case is another text book example of a fundamental "turn of the century" need for statutory and regulatory legal reform of medium specific requirements. These reforms need to occur within each jurisdiction in which the medium specific laws creating barriers to commerce currently exist. That means states need to reform our areas of existing jurisdiction and the federal government must clean its own house. I believe it would be unwise and unwelcome for our federal partners to view the need for such law reform as an opportunity to change the underlying balance of substantive jurisdictions between states and the federal government.

Just identifying these laws is quite difficult, but drafting the best language to selectively repeal or amend them to be consistent with appropriate methods will take even more work. There are some 4,515 such requirements in the Massachusetts General Laws alone! It will take some time to reform each law and regulation - probably several years. In the meantime, an early Act at the federal and state levels respectively that reforms the easy to handle laws in a clean sweep and statutorily instructs the judiciary and any other adjudicative body to interpret remaining requirements to be consistent with information age practices would be an excellent first step.

My sense is that such a "base-line" legal reform would be appropriate to take place in the near-term - even before report of the Uniform Electronic Transactions Act by the National Conference of Commissioners on Uniform State Law (NCCUSL) which will deal with far more complex issues. This Act is due out in a couple of more years or so. Meanwhile, states are already converging on an "electronic signature" consensus - the vast majority of legislation enacted at the state level merely creates "equivalence" between paper and electronic media for writings and signatures. The recent excellent Internet Law and Policy Forum legislative survey confirms this trend.

I remain unconvinced that there is a need for federal preemptive law in this area. However, to the extent federal law in this area may end up preempting state law, Congress should attempt some creative solutions to the issue; such as drafting a broad federal "electronic signature and records" law with a provision that states shall enact "similar" or "consistent" uniform law within x time. Tthis would not be unprecedented - look, for example, to the Money Laundering federal law that explicitly pointed to NCCUSL to write uniform law on non-depository institutions to fill out the federal law or look to the real-life political formula between the states and the federal government that led to Article 4A.

Another more aggressive and probably more problematic approach would be for the federal law to apply equally to federal and state law (effectively just eliminating state writing and signature requirements that fall within the scope of the law) but then providing that the law shall not take effect until the year X and that states may enact law that further defines, expands or, if necessary for an important public interest, limits the federal law - provided that the state laws are sufficiently uniform and consistent with the federal law and that any statute that is meant to modify the federal law explicitly so state within the body of the statute (so everyone can see exactly what law applies in this regard). That would allow states to either go along with the federal treatment of the issue - assuming it was adequate - or to arrive at a superior treatment that takes account of the several unique issues that arise under state jurisdictions.

Under the latter approach, if states were to do nothing - then the federal law would govern. Similarly, if states were to enact inconsistent law - then the federal law would preempt by its own terms. Under either approach, if the states were to act in some unforeseeable manner that had the effect of disturbing interstate commerce, then the federal government would always retain power under the commerce clause to enact preemptive law once and for all. However, it seems to me that we are in a period of transition and that law or policy makers at all levels of government would do well to cut each other some slack and a bit more time to come up with creative, well thought out and tailored solutions to accomplish the legal reforms that are needed. Under either possible preemptive solution explored above, and just in general, state and the federal government must talk to each other about what we are doing in this fast moving area to assure adequate coordination - including coordinating approaches where we agree not to act - that is, to keep our grasping hands off from the marketplace (that is my favored government action).

I am dubious about the merits of federal activism in the area of electronic authentication that preempts state law or intrudes on the market. Clearly all levels of government need to reform existing law so as to remove barriers to commercial and other societal uses of information technology. Beyond that, federal law should leave states and the market alone to the maximal extent practicable. The core constitutional scheme blessing the American people with a system of state and national government comprising separate powers and jurisdictions has been an extremely helpful innovation in the course of western civilization. It is working out quite well for the country so far and we should tamper with it only based on a showing of great need and a period of long deliberation. The balance or separation of power works and has saved us from the occasional but cyclically recurring bizarre mania associated with federal policy makers from generation to generation (e.g. McCarthy) and has also prevented the worst excesses at a state level from persisting against the conscience of the country (e.g. racist state laws).

Issues central to electronic authentication and records include contracts, commercial law, rules of evidence in state courts, state chartered financial institution regulation, and many other areas of primary (or exclusive) state jurisdiction. Several other bodies of law, such as consumer protection, privacy and an array of records retention rules comprise areas of state jurisdiction that are concurrent with that of the federal government. Here to, further incursions into the areas of states interests should be undertaken with care, discretion and mature restraint. The sovereignty of our American states has been slowly diminished over the decades to feed an increases in federal expansion. The prospect of yet another fundamental shift in jurisdictions from the states to the federal government - this time in the realm of electronic authentication and records - would leave precious little to the states as our civilization crosses the brink to ubiquitous use of information technology systems.

If the Kaspar case shows anything, it is that many complicated areas of law exist that will require time to reform for the information age. The stampede which has grown in strength over the past year for "over-arching federal law" in the "short term" may be headed toward a cliff. Proponents of such law often seek liability limits, government regulation or oversight, aggressive preemption of state law and substantial reversal of evidentiary presumptions. Such radical interference with the market and the careful balance between levels of government, though probably constitutional, would definitely be premature and prone to severe unintended consequences. Federal government review boards with punitive regulatory powers or other similar industrial-planning attempts would stymie a market that needs time to grow. The market distortion following such a move would chill innovation and lead toward a culture of "compliance" with the federal standards (rather than more appropriate market-based standards). Merely having private sector members of government regulation schemes does not create a market environment. No market has ever been regulated into existence - and no government will succeed in such an effort. Healthy, worthy markets arise as a result of the interplay of supply and demand.

The Kaspar court noted only that " in this instance the law lags behind technology and custom." The judge was wise in this respect indeed. He did not indicate that "new law is needed to create predictable legal outcomes" or that "we need new law to set the framework for electronic commerce." Evidently, the judge would be quite capable of applying existing law and reaching equitable and predictable results under this - or any other - substantive area of law. The judiciary is being held back not by the lack of new law for an information age - but by the existence of old law from the industrial and agrarian ages that specifies media that no longer make any sense. The emergence of business practices and technological deployments to meet the demands of the market will evolve without special laws or government actions to "spark" the market. Simply removing the impediments will allow the flame to grow, but enacting new laws that reach into the market or upset the American separation of powers may result in dousing the fire and creating other problems as well. States and the federal government would do well to take the court's advice at face value by focusing our attention on matching the law to technology and custom - and no more. As sound business practices and technologies come into wide spread use, the law should take care to validate, enforce and otherwise support commercially reasonable expectations.

The judge, by requesting reform of federal law to remove barriers and simultaneously refusing to step ahead of truly wide spread practices or statutory rules of construction has articulated a direction for legislatures and markets alike. This may be one of the ultimate expressions of our judicial system's role - deciding a given case on its merits with a mature, restrained communication of wisdom. Will we accept it?

Daniel Greenwood practices information technology law for the Commonwealth of Massachusetts and holds an academic appointment as lecturer at Massachusetts Institute of Technology where he teaches at the graduate level on topics of electronic commerce and virtual communities.
dan@civics.com
www.tiac.net/biz/danielg