AMERICAN BANKERS ASSOCIATION

CERTIFICATION AUTHORITY
LIABILITY ANALYSIS

(February 1998)

Thomas J. Smedinghoff
Wildman Harrold
225 W. Wacker Drive
Chicago, Illinois 60606
Phone: 312-201-2021
Fax: 312-416-4773
smedinghoff@wildman.com

CERTIFICATION AUTHORITY LIABILITY ANALYSIS

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

This memo surveys the liability issues raised by an entity's entry into the certification authority business.[1] It is, however, in many respects an uncharted territory. As one commentator has noted " the duties and potential liabilities imposed upon a CA by U.S. law are unclear, as might be expected from the dearth of applicable legislation, the complete absence of case law, and the very small number of currently functioning CAs."[2] Accordingly, this memo addresses the major sources of law likely to provide a basis for certification of authority liability, and analyzes those areas of the law in analogous situations in an attempt to determine how they might be applied to the activities of a certification authority.

The focus of our efforts was on what appear to be the four primary areas of potential liability: negligent misrepresentation, breach of warranty, intellectual property infringement, and liability for the conduct of others. That is not to imply, however, that there are not several other areas of law and legal theories that might support a finding of liability against a certification authority. Other bases of liability might include antitrust, interference with contractual relationships, unfair competition, and defamation.

Engaging in the business of a certification authority involves entering a type of business to which the law has not yet had time to adapt. By issuing digital certificates that verify identity, a certification authority is, in essence, engaged in the business of an information provider. This is, in many respects, different from traditional businesses that involve the sale of goods, or traditional businesses that involve the provision of services. Moreover, while publishing industries have engaged in providing information, issuing digital certificates is significantly different because of the fact that they are intended to be relied upon by parties to a commercial transaction. It is this aspect of reliance that is critical. Both the certification authority that issues a certificate and the subscriber that acquires it do so with the intention that it will be used by third parties to verify identity and engage in business transactions. In fact, that is the very nature of a certificate.

Given the fact of this intended reliance, the critical issue for a certification authority becomes the accuracy of the certificate. Stated otherwise, what is the CA's liability for errors in the certificate, errors in a repository containing certificates, or errors in a certificate revocation list ("CRL") on which third parties rely to their detriment? Thus, the primary focus from a liability perspective is on the tort of negligent misrepresentation and contract actions for breach of warranty that are either express or implied regarding the accuracy of the information provided. Relatedly, it is also necessary to consider intellectual property issues that permeate the certification authority process. And finally, for an entity that intends to outsource a large part of its certification authority obligation to a certificate manufacturing authority, it is important to

---

[1] This study was originally prepared in February 1998. Participating attorneys were Thomas J. Smedinghoff, Andrew R. Basile, Ruth Hill Bro, John Murphy, and Andre Frieden.

[2] A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce,* 75 OR. L. Rev. 49 (Spring 1996).

consider the liability for the conduct of the third persons acting on its behalf that might also cause injury.

The following is a summary of the findings set forth in the sections that follow in the Memorandum.

1.1 Tort Liability -- Negligent Misrepresentation

When operating as a certification authority, ("CA") an entity will primarily be in the business of providing information, in the form of certificates, a repository, and a CRL. To the extent such information is incorrect due to the failure of the CA to exercise reasonable care, the CA will be liable for the tort of negligent misrepresentation to persons who rely on the information to their detriment.

Negligent misrepresentation creates a duty to exercise reasonable care to verify facts, but it does not make the CA a guarantor of the accuracy of the information provided. The CA is subject to liability only if the error results from its negligence.

Understanding the scope of the CA's potential liability for negligent misrepresentation requires consideration of two basic issues: (1) what is the legal duty, if any, owed by the CA; and (2) to whom is such duty or obligation owed?

The extent of the legal duty owed by one person to another is described as the standard of care. The standard of care to be exercised in any particular case depends upon the surrounding circumstances and the extent of foreseeable danger. There are five possible standards of care that may apply to an entity's activities as a certification authority: (1) a general standard of ordinary or reasonable care; (2) a professional standard of care; (3) a strict liability standard; (4) a statutorily-mandated standard; and (5) possibly, a standard measured against criteria established by the CA itself.

At present, it appears that CAs will most likely be held to a general standard of reasonable care. From a business perspective, reasonable care means that degree of care that an ordinarily prudent person engaged in the same line of business would exercise under similar circumstances. Unfortunately, in an industry as novel as that of the certification authority, there is no established standard of care. Appropriate standards of reasonable care take time to be established, and are based in part on the customs of the industry, what people have come to expect, and what courts will allow based on the goal of tort law to remedy harm to individuals. The fact that CAs, by their nature, will be parties with specialized skills in whom laypersons place trust beyond that of the normal marketplace may eventually give rise to professional status, or otherwise subject them to a higher duty of care to do what is reasonable given their specialized skills.

Generally, it appears that a CA will not be permitted to set its own standards of care. A minimum standard of care applies with respect to any given activity. In most cases it is likely to be a reasonable care standard, measured by the extent to which a company's practices meet or exceed what seems reasonable in light of the risk involved in a given activity, although in some

cases standards of conduct may be set by statute. For example, the Utah Digital Signature Act imposes various duties upon a licensed CA in connection with the issuance of certificates concerning identification of the parties to the certificate, the security of the private key, and the functioning of the public key. Generally, the CA will need to carefully consider the anticipated use of the certificates it issues, and ensure that its procedures are appropriate to protect against harm to others arising from those uses.

The second issue concerns to whom a duty or obligation is owed? A CA potentially has tort duties with respect to three groups of people: (1) subscribers (i.e., the persons to whom certificates are issued), (2) parties relying on certificates, repositories, and CRLs issued or maintained by the CA ("relying parties"), and (3) third party victims of fraud. Whether it actually owes a duty to each of these classes will vary depending on the jurisdiction, since liability often depends on the nature of the relationship between the information provider and the party whose reliance resulted in loss. In the identifying third parties to whom a CA owes a duty of care, courts generally take one of three approaches:

> (1) Foreseeability Standard: One will be liable to any person for whom reliance on the false representations was reasonably foreseeable. This is the broadest standard of liability applicable to information providers.
>
> (2) Standard Based on Intent and Knowledge: There is a more limited scope of liability, providing that liability is limited to loss suffered (a) by a member of the group of the persons for whose benefit and guidance one intends to supply information or knows that the recipient intends to supply it; or (b) through reliance upon it in a transaction that he intends the information to influence or knows that the recipient so intends, or in a substantially similar transaction. This standard is the most widely adopted.
>
> (3) Privity Standard: This is the most limited standard, creating a duty owed solely to the client, or one with whom the information provider had specific contact. Some states adopt this approach as a matter of common law while others adopt statutory applications.

In addition to liability for incorrect information based on negligent misrepresentation, there also exists the possibility that the use of a CA's branded certificates (or the CA's logo) by subscribers may be construed as an endorsement of the subscriber by the CA in a manner that may lead to liability. Endorsers of products may be liable for negligent misrepresentation if the product fails to live up to the justifiable expectations of quality created by the endorsement and a consumer is harmed by relying on that endorsement. Independent testing laboratories, magazines that endorse products, and trade associations which lend their mark to products have all been held liable for negligent misrepresentation when the products failed to meet expectations. A certificate itself may be considered an endorsement by the CA of the subscriber or web site that it is used to verify, which may make the CA analogous to an endorser. As a general matter, endorsers may only be held liable to the extent of their representation, and only if the plaintiff could prove that the endorser was negligent in making that representation. The CA

might reduce the potential for such liability by carefully delineating the nature of the representation it is making with respect to the certificates it issues.

A CA's liability for tort claims based on negligence may be limited by the so-called "economic loss doctrine." The economic loss doctrine provides that claims for purely economic losses based on product defects are not recoverable in tort. The rule holds simply that tort liability does not arise for pure economic loss, but only for personal injury or property damage. The principles behind this rule are that protecting personal injury and property damage claims are more important social policies than pure economic (business) losses, and that economic losses are better protected by negotiated contract allocations rather than through generalized tort law. While the economic loss rule is not universally adopted, its influence extends broadly into the majority of states and is growing. Some states apply the doctrine to services and to negligent misrepresentation claims, and some states provide exceptions to the doctrine, which may allow tort claims for purely economic losses. Some states do not apply the doctrine at all. There is little consistency as to how it is applied from state to state. However, because of the financial nature of losses likely to be suffered by users of certificates improperly issued by the CA, the CA may be protected from third party tort actions for economic losses in those states that preclude recovery in tort for purely economic losses based on negligent misrepresentation.

By using notices and disclaimers to define the scope of the product or services they provide, information providers may be able to put third parties on notice that any reliance on the information contrary to the notice or disclaimer may be unreasonable and thus may be undertaken at the relying party's own risk. While disclaimers will not necessarily overcome liability for intentional fraud, they may be effective to limit liability for negligence by controlling questions about the justifiability of a party's reliance. Because reasonable or justifiable reliance on provided information must be shown in a negligent misrepresentation case, the general effect of such a disclaimer may be to put third parties on notice that any reliance contrary to the disclaimer may be deemed unreasonable and thus preclude recovery in the event that errors occur.

Unfortunately, unlike an accountant's opinion letter, which can easily accommodate a conspicuous disclaimer, digital certificates are not nearly as flexible. A certificate may only be able to incorporate a disclaimer by reference. CAs may be able to contractually bind third parties to exculpatory clauses by requiring subscribers to incorporate such provisions in their contracts with third parties. However, it remains unclear whether CAs could rely merely on a non-contractual disclaimer to limit their potential liability to third parties for negligent misrepresentation liability.

Assuming that a non-contractual disclaimer by a CA is effective, then the issue becomes one of notice. Given the limited space on a certificate, and given that a relying party may not even see the certificate itself, providing adequate notice of the disclaimer to relying parties may prove difficult.

1.2 Contract Liability

A CA's contractual and warranty obligations depend, in part, on what law applies to its certification authority activities. Article 2 of the Uniform Commercial Code (UCC) governs transactions in goods, the common law (judge-made law) applies to transactions in services and to contracts pertaining specifically to the provision of information, and Proposed Article 2B (a revision of the UCC that could be approved within the next year) applies specifically to the licensing of information.

Many of the CA's proposed activities, such as maintaining a repository and CRL and receiving, transmitting, revoking, suspending, and managing certificates, appear to be services and thus subject to the common law (court-made law). Other of the CA's proposed activities, including issuing certificates and authenticating subscribers, could be characterized as provision of either a service or a good and thus be subject, respectively, to the common law or to the Uniform Commercial Code (UCC), the latter of which governs transactions in goods. Yet, even when a commercial activity does not directly fall under the UCC, courts will often refer to it as persuasive authority. Because a CA's proposed activities largely constitute the provision of information, the common law and Proposed Article 2B could also be key to determining the CA's potential liability to subscribers, relying parties, and impersonated third parties.

UCC law governing contracts for *goods* is very results-oriented -- certain default warranties and other obligations arise under a UCC-governed contract to ensure that the product conforms to ordinary standards of performance. Parties are free to agree otherwise on many points and thus can limit or exclude most warranties, limit remedies, and impose damage caps and other limitations on liability. Even when parties can bargain for different contract terms, certain UCC rules restrict the ways in which they disclaim or limit their liability. By and large, disclaimers and other liability limits must be conspicuous (a notice sort of issue), which raises special problems in an electronic context, particularly with regard to digital certificates. Other provisions of the UCC cannot be disclaimed. In particular, regardless of the terms of the contract, the UCC will impose an obligation of good faith, diligence, care, and reasonableness. The UCC also will not tolerate unconscionability -- i.e., a surprise term that no one in his right senses would accept -- especially when an unsophisticated consumer could be hurt.

The common law governing contracts for *services* is more process-oriented. Courts ask whether the provider of the service performed in a reasonably careful and workmanlike manner, especially in light of the particular trade or profession from which the service provider is drawn and of the abilities, skill, and knowledge claimed by that service provider. Because those who provide services often must deal with factors beyond their control, courts tend not to read into contracts express and implied warranties that amount to "insuring" or "guaranteeing" favorable results, unless the parties have expressly agreed to that higher standard (which often entails the payment of a higher price). Alarm/security companies, title searchers, inspectors, and others are not expected to produce infallible results; instead, they are expected to adhere to certain procedures depending on the circumstances. Likewise, *information providers* typically are not required to ensure 100% accuracy. This is especially true for those who publish for a mass-market, as a newspaper does. As the relationship between the parties gets closer, and the

information provider has more reason to know of the relying party's particular needs and is compensated accordingly, the obligations regarding the provision of information increase.

Courts generally uphold exculpatory clauses that limit a party's liability under a contract unless they violate public policy or something in the social relationship between the parties dictates against it. For example, exculpatory clauses that exempt a party from tort liability for physical injury, or harm that was intentionally or recklessly caused, violate public policy, while clauses that exempt a party for its own negligence usually are enforced. Key to this presumption, whether under the UCC or the common law, is that the parties have bargained for this provision and the price has been set accordingly. This is particularly true with regard to services: those whose payment is based on the service rendered (not on the value of the property at issue) cannot be expected to act as an insurer if the service fails to prevent a substantial loss, such as where an alarm fails to go off and the thief steals all of a company's computers or where a CA fails (either because it was negligent in following its procedures or because the procedures -- however reasonable in the trade -- were insufficient) to identify an impostor in issuing a certificate, resulting in substantial financial loss.

Courts are divided as to whether one can exclude one's own liability with respect to third parties who are the intended beneficiaries of a contract. In the case of a CA, the relying parties arguably would be third-party beneficiaries of the contract between the certificate authority and a subscriber bank. Many courts hold that a third-party beneficiary's rights are no greater than those of the party from whom the rights are derived; if limits on liability apply to the subscriber, they should also apply to the beneficiary, or so the argument goes. One way of helping to make this outcome more likely is to avoid making promises that guarantee certain results, to impose limits on liability while leaving some remedy in the event the contract is breached or an obligation is not met, and to draft the contract so that it does not extend to third parties (or at least get indemnification from the subscribing bank if a warranty or obligation is deemed to extend to third parties). Releases from third parties could also potentially exculpate the CA for any negligence, but because the CA's contact with third parties is somewhat indirect, this may be difficult to achieve. To the extent that a CA can characterize its activities as provision of a service, as opposed to provision of a good, its flexibility in achieving these objectives will be enhanced.

Although becoming a licensed certificate authority pursuant to a state digital signature statute such as the one enacted by Utah can provide a safe harbor with regard to potential liability, such a statute can also impose significant obligations and give rise to certain warranties. Likewise, although proposed UCC Article 2B affords significant protections to information providers (and perhaps a more predictable result because it is oriented to electronic media), it also imposes different default rules and obligations in some instances to which a CA could become subject.

Consumers may constitute a large number of the relying parties. If certain consumer statutes apply to these transactions, this could restrict a CA's ability to limit its obligations and potential liability. In all likelihood, however, a CA can effectively reduce its potential liability through careful use of contractual language and representations it makes in its CPS, advertisements, and the like.

1.3 Statutory Liability -- Digital Signature Regulation

One potential source of liability for a CA may arise through statute, specifically from the application of provisions contained in digital signature legislation and administrative regulations promulgated pursuant thereto. Such regulation exists, or may soon exist, not only in the various states, but also at the federal and international levels.

To date, some form of digital or electronic signature legislation has now been enacted or is currently being considered in 47 states.[3] The form and scope of this legislation varies widely. Of these states, nine have enacted or are currently considering comprehensive digital signature acts that embrace the concept of a certification authority and specifically address liability issues. Other less comprehensive acts expressly authorize the use of digital or electronic signatures either generally or in connection with communications with the state government, but may or may not expressly contemplate the use of certification authorities or specifically address liability issues. Still others merely authorize the use of digital or electronic signatures in connection with a specific context, such as filing tax returns or corporate documents with the state government, and do not specifically address certification authorities or their liability. It is difficult to gauge at this time the extent to which future legislation might affect the liability of certification authorities, or the extent to which it could impose regulatory burdens.

The Utah Digital Signature Act (the "Utah Act") was the first comprehensive digital signature act to be enacted and has since been used as a model by other states.[4] The Utah Act establishes a voluntary licensing program for certification authorities. Certification authorities who voluntarily subject themselves to the Utah Act must comply with the various duties imposed upon them in connection with, among other things, the issuance and revocation of certificates and the maintenance of a repository. Failure to comply with these statutory duties could not only trigger administrative enforcement action, but also could serve as a basis for negligence liability in tort.

On the other hand, the Utah Act also helps to *limit* the amount of potential liability in some ways too, such as by capping the liability of a *licensed* certification authority under certain circumstances at the amount specified in the certificate as the recommended reliance limit. The Utah Act also expressly limits the types of damages available to third parties who incur losses in connection with their reliance on a certificate.

One example of the duties imposed by the Utah Act are those duties that arise in connection with the issuance of a certificate. Certification authorities licensed in Utah may issue a certificate to a subscriber only after various conditions have been satisfied. Those conditions include, among other things, that the certification authority has confirmed that: the prospective subscriber is the person to be listed in the certificate to be issued; the information in the certificate to be issued is accurate after due diligence; the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate; the prospective

---

[3] A regularly updated summary of this legislation is available at *www.bakernet.com/ecommerce*.

[4] Washington and Minnesota have enacted similar statutes.

subscriber holds a private key capable of creating a digital signature; and the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber. Certification authorities licensed in Utah are also required to use only a "trustworthy system" and must disclose their certification practice statement.

Although only certification authorities licensed in Utah (or in states with similar digital signature legislation) are subject to these statutory duties, such legislation nevertheless may serve as a model for measuring the reasonableness of a certification authority's conduct in states where such statutes do not yet exist. Thus any certification authority would be well advised to take these and other statutory standards of care under consideration when establishing the procedures to which it will adhere in connection with offering certification authority services.

As of yet there has not been any federal legislation enacted specifically pertaining to certification authorities. However, federal regulation of certification authorities may not be very far away. One bill recently considered in Congress would establish a national association of certification authorities to which any person or group wishing to provide electronic authentication services in the United States would have to belong. The Bill would also create a standards review committee to establish and refine criteria to be applied to the emerging electronic authentication industry. This committee also would be charged with establishing and adopting guidelines, standards and codes of conduct applicable to certification authorities. Thus, the possibility exists that at some point in the future certification authorities could become subject to potentially extensive and burdensome federal regulation.

1.4 Intellectual Property Liability

Intellectual property is a set of legally-recognized rights in intangible subject matter such as inventions and trademarks. These rights include patents, copyrights, trade secrets, and trademarks and related rights arising under unfair competition law and privacy. Activities of a CA that violate intellectual property rights of another party are said to *infringe* the other party's rights. Depending on the right infringed, remedies for infringement may include damages, profits, punitive damages, attorneys' fees and injunctions against further infringement.

Patents. Patents may cover technology used in a CA's business including software, encryption and security procedures. If a CA infringes a third party patent, it will be liable for damages (which may be trebled in cases of intentional infringement), subject to an injunction and potentially required to pay the patentee's attorney's fees and costs.

We are aware of some significant patents held by RSA Data Security which will probably impact a CA's operations. Other pertinent patents may be uncovered by commissioning an infringement study. To the extent that a CA outsources a significant portion of its CA business to a third party, it may be able to look to such third party to shoulder the primary burden of ascertaining what patents may be infringed and obtaining appropriate licenses from the patent holders. To protect itself, a CA should insist on an indemnity from the third party in the event a third party claims patent infringement. Note that the CA will retain some functions, and in performing these retained functions, the CA may have third party infringement problems that are not covered by the third party's indemnity.

Copyrights. Copyright protects original works of authorship fixed in a tangible medium of expression. Copyrightable subject matter includes text, photographs, drawings and computer code. The CA deals with many copyrightable works, including software and documentation, the repository, and other databases, and potentially the format and content of a certificate. Copyright protects the expression of ideas, but not the ideas themselves. Thus facts, systems, and ideas are not protected by copyright.

A copyright owner is entitled to recover actual or statutory damages. Actual damages are damages suffered by the copyright owner as a result of the infringement and any profits of the infringer that are attributable to the infringement and are not taken into account in computing the actual damages. A court may also award costs and attorney's fees to the prevailing party in a copyright lawsuit and grant temporary and final injunctions to restrain further infringement.

To avoid infringement issues, a CA should either develop its own software, documentation and databases, acquire the copyrights to these materials if they are developed by others, or enter into suitable license agreements with these parties to use the materials. As with patents, should insist that third party outsources and indemnify it against claims by others of copyright infringement for copyrightable works developed and/or used by the outsourcer in performance of its agreement with the CA.

Trade Secrets. A trade secret is generally defined as "information .... that: (a) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality."

CAs may potentially receive trade secrets from vendors (e.g., in software) and subscribers (e.g., in certificate applications). These disclosures may in most instances be made pursuant to some type of written confidential disclosure agreement, which may have the effect of supplementing or limiting the disclosing party's rights under trade secret law. Anytime a CA is entrusted with trade secret or other confidential information of another party, it has potential liability exposure if the information is misused or not properly secured. A CA should implement procedures and policies for managing this risk.

If a CA misappropriates a trade secret it may be liable for damages, required to pay a reasonable royalty for continued use of the secret or enjoined from using the secret. Under the recently-enacted Economic Espionage Act, trade secret misappropriation may also bring criminal consequences to the CA and the individuals involved in the misappropriation.

Trademarks. Trademarks are words, symbols or other devices used to distinguish the goods or services of one person from those of another. Everyday examples include "Ford" for automobiles and "IBM" for computers. The owner of a trademark has the exclusive right to use the mark in a particular market on particular kinds of goods or services. A federal statute known as the Lanham Act provides remedies to trademark owners for infringement of their rights. These remedies include damages, disgorgement of the infringer's profits, and injunctive relief.

Trademark law may impact a CA in two ways. First, the CA will presumably market its CA services under a brand name. In doing this, the CA should ensure through an appropriate study that the use of that brand does not infringe a prior user's rights.

Second, certificates issued by a CA may contain references to third-party trademarks, particularly in the *organization name* field of the subscriber's *distinguished name*. For example, a certificate might be issued to the organization "First National Bank." Issuance and use of this certificate may raise trademark and unfair competition issues with respect to the owner or owners of the mark "First National Bank."

Our concern in this regard is that the CA may be liable under the Lanham Act to third parties whose marks have been misappropriated in CA certificates issued at the request of impostors. Most troubling in this regard is that trademark liability, if applicable, does not require the CA to have acted negligently or with bad intent. Once the certificate is issued containing the trademark, liability may arise.

Fortunately, the Lanham Act provides an "innocent infringer" defense. It is not clear whether this defense would be available to a CA, however. Even if available, the defense requires the CA to have acted objectively reasonable in determining that the subscriber of the certificate was authorized to use the mark at issue.

Overall, the Lanham Act, as it applies to erroneously issued certificates, raises a number of concerns that we have not yet definitively resolved, and we recommend that this area be given further study.

1.5 Liability for the Conduct of Others

Many (and perhaps most) of the injuries that may flow from or relate to the activities of a CA are likely to be caused not by the corporate persona of the CA, but rather by the CA's employees, contractors, subscribers and other third parities. Even though the CA is not directly at fault in these instances, it may be liable for the torts and crimes of others under theories of (a) vicarious liability, (b) agency, (c) contributory infringement, (d) corporate negligence, and (e) liability for the criminal conduct of a third party.

Vicarious liability (or *respondeat superior)* is generally defined as the imposition of liability upon one party for the wrong committed by another party. Under this doctrine, the CA may in many instances be liable for negligence, intentional torts and crimes of its employees that are committed within the scope of their employment. Put in other words, the tort or crime of the employee may be imputed or attributed to the CA. For example, if a CA employee intentionally issues an erroneous certificate for the purpose of defrauding a third party, the CA will be liable. The fact that the employee is acting for his own purposes will probably not relieve the CA of liability if the CA has provided the opportunity for the employee to commit the fraud by entrusting to him responsibility for issuing certificates.

The CA may also be vicariously liable for the conduct of its independent contractors with respect to their performance of the CA's *non-delegable* duties. A *non-delegable* duty is a duty

from which a person cannot absolve himself by simply delegating it to another. For example, the duty of a landlord to maintain common areas and the duty of a railroad to maintain safe crossings have been considered non-delegable. It is not clear which duties of the CA would be non-delegable, but a safe assumption would be that a CA's core responsibilities (i.e., complying with the CPS and securely maintaining the CA private signing key) are non-delegable.

The CA may also be liable for the conduct of its suppliers to the extent they are acting as the CA's agents. Agency is a fiduciary relationship in which one person (the agent) acts on behalf of and subject to the control of another person (the principal). While a servant (be he a janitor or an executive) is always an agent, an independent contractor may or may not be an agent depending on the circumstances. A relationship with a CMA will probably create a limited agency relationship. This means that the CMA can potentially create substantial liability for a CMA, particularly if its misuses the CA's private CA signing key.

In sum, the a CA will probably be legally responsible under agency principles for any act that a CMA performs using the CA's private key assuming that the CA entrusts its key to a CMA for the purpose of issuing certificates on behalf of the CA. This is also true with regard to any intentional fraud perpetrated by the CMA or its employees.

Apart from its contractors and employees, the CA may be liable to third parties for certain tortious or criminal conduct on behalf of its subscribers. Suppose, for example, that an impostor posing as the First National Bank obtains an erroneously issued certificate from the CA and uses that certificate to perpetrate a fraud on a relying party. The impostor has committed a tort (fraud) against the relying party and potentially other torts (false impersonation and unfair competition) against the party whose identity has been appropriated. In some circumstances, the CA could be liable in negligence if it failed to take reasonable precautions to prevent the intentional conduct of the impostor. It is also possible the impersonated party may have a trademark claim against the CA.

Overall, the CA should be aware that it may be legally accountable for the use (and misuse) of its CA services by CA employees and contractors.

1.6 Recommendations for Managing Liability Risk

A summary of recommendations for avoiding or limiting liability exposure is set forth in Section 9 of the memo.

1.7 Strategies for Protecting Intellectual Property Rights

Intellectual property rights were first considered from a liability perspective (*i.e.*, how intellectual property rights of others may impose liability on a CA). It is also important to consider how intellectual property rights can be used to protect the CA's intangible assets. We focus first on subject matter that can or cannot be protected by intellectual property rights and the procedures by which the CA can acquire these rights. We then apply these general principles to the documents, brands and technologies that may be used in the CA 's business.

Patents. Patent protection is available for software and other technology developed by or for the CA that is useful, new and nonobvious. The patent law does not protect discoveries of the laws of nature, physical phenomenon, algorithms or abstract ideas by themselves. If there is anything patentable from such discoveries, it is the application of the natural law, phenomenon or idea to some new and useful end.

Patents are available throughout the world, and are issued on a country-by-country basis. Patents are obtained in the U.S. by filing a patent application with the federal Patent and Trademark Office ("PTO"). Patents in foreign countries are similarly obtained by filing an application in each specific country. Applications must be filed within a one-year statutory bar period that can be triggered by various events including the first sale or offer of sale of the invention. Because patent applications must be filed by the individual inventors, it is important that the CA have in place employment or contractual relationships with the inventors to ensure that the CA owns the patent.

Copyright. Copyright protects "original works of authorship, including software and documentation. All such works are automatically protected by copyright from the moment they are created and expressed in a tangible medium, such as on paper or on a computer disc. No further actions are strictly required, although registration with the U.S. Copyright Office is highly beneficial.

Copyright is not available for specific facts, but can arise in a compilation of facts if the selection and arrangement of the facts constitutes an original and creative work of authorship. Thus some databases may be protected by copyright. Others, such as a standard white pages directory, lack the requisite originality and are therefore not protected.

If the CA uses independent contractors to create copyrightable works (including a CMA), it should have a written agreement with the contractors specifying that the CA-- and not the contractors -- owns the work product, and assigning all rights to the CA.

Trade Secrets. Trade secret protection for information, like copyright and trademark protection, applies automatically to information that qualifies. No legal formalities such as notice or registration are required. However, as discussed below, there is a general obligation to take steps that are appropriate under the circumstances to keep the information secret. Thus, the CA must establish confidentiality agreements with everyone who will have access to trade secret information. Confidentiality agreements can also be used to protect information -- such as private keys -- that might not fall within the statutory definition of trade secret.

Trademarks. A trademark is a word or symbol that is used in connection with goods and services in commerce to distinguish them from the goods and services of others. The CA will want to develop trademark rights in the brand under which it markets its CA services. This is a three-step process. First, the CA should select a name that is distinctive, and not merely descriptive. If the brand is descriptive (e.g., "Digital Signature Partners"), it will be difficult for the CA to develop rights in the brand. Second, the CA should conduct a clearance study to determine if the name is available. Third, if the name is available, the CA should file trademark

registrations in the U.S. and, if desired, foreign countries. To the extent practicable, the CA should ensure that any domain name used in connection with its service is also registered by the CA with the U.S. PTO.

Candidates for Protection. Using the intellectual property rights described above, the CA can develop strategies for protecting aspects of its CA business, including:

- *Databases* such as repositories and CRLs
- *Documentation* such as the CPS and user manuals
- *Brand names* under which the service is offered
- *Software* used to provide the service
- *Content* of a particular certificate
- *Format* of certificates, including data structure
- *CA Key Pairs*
- *Interfaces*, particularly user interfaces
- *Encryption methods* and other security procedures

2. FUNCTIONS OF A CERTIFICATION AUTHORITY

2.1 Overview of Digital Signatures

For electronic communications to be viable, from both a legal and a business perspective, the messages that are exchanged and the records that are preserved of these communications must satisfy certain legal requirements. While not all of these requirements will apply in every situation, they generally include the following:

- Authenticity
- Integrity
- Nonrepudiation
- Writing and signature

Authenticity is concerned with the source or origin of a communication.[5] Who is the message from? Is it genuine or a forgery? A party entering into an online contract must be confident of the authenticity of the communications it receives. For example, when a bank receives an electronic payment order from a customer directing that money be paid to a third party, the bank needs to be able to verify the source of the request. The bank is faced with the problem of ensuring that it is not dealing with an impostor.[6]

Integrity is concerned with the accuracy and completeness of the communication. Is the document the recipient received the same as the document that the sender sent? Is it complete? Has the document been altered either in transmission or storage? The recipient of an electronic message needs to be confident of a communication's integrity before he will rely and act on it.

Nonrepudiation is concerned with holding the sender to his communication. The sender should not be able to deny having sent the communication if he did, in fact, send it, or claim that the contents of the communication as received are not the same as what the sender sent if, in fact, they are what was sent. Nonrepudiation is essential to electronic commerce when it comes to a trading partner's willingness to rely on a communication, electronic contract, or funds transfer request. For example, a stockbroker who accepts buy/sell orders over the Internet would not want his client to be able to place an order for a volatile commodity, such as a pork bellies futures contract, and then be able to confirm the order if the market goes up and repudiate it if the market goes south.[7]

Writing and signature requirements are, in essence, legal formalities. In many cases applicable statutes and regulations require that an agreement be both (1) documented in

---

[5] *See* Fed. R. Evid. 901(a) (1995).

[6] *See* U.C.C. §§ 4A-202, 4A-203 & Official Comment.

[7] *See generally,* "Follow the Money--A New Stock Market Arises on the Internet," Scientific American 31 (Jul. 1995).

"writing" and (2) "signed"[8] by the person who is sought to be held bound in order for that agreement to be enforceable.

For electronic communications, digital signature technology offers one of the most promising information security measures available to satisfy the legal and business requirements of authenticity, integrity, nonrepudiability, and writing and signature. Digital signatures are based on a form of encryption technology known as public key cryptography. In public key cryptography, each user generates an encryption key pair consisting of two very long numbers known as keys. These keys have a special mathematical relationship in that any message encoded with one key can only be decoded with the other key. All keys and key pairs are unique -- no two keys are identical.[9]

Before a sender can digitally sign an electronic communication, the sender must first generate a key pair using appropriate software. One of the keys is designated as the "private key" and the other key is designated as the "public key." The private key is kept confidential by the sender, and is used for the purpose of creating digital signatures. The public key can be disclosed generally by posting the key in online databases, repositories, or anywhere else the recipient of the digitally signed message can access it.

To digitally sign an electronic communication, the sender runs a computer program that creates a unique message digest (or hash value) of the communication. The program then encrypts the resulting message digest using the sender's private key. The encrypted message digest is the digital signature.[10] The sender then attaches the digital signature to the communication and sends both to the intended recipient.

When a recipient gets a digitally signed communication, the recipient's computer runs a computer program containing the same cryptographic algorithm and hash function the sender used to create the digital signature. The program automatically decrypts the digital signature (the encrypted message digest) using the sender's public key. If the program is able to decrypt the digital signature, the recipient knows that the communication came from the purported sender, that is, the recipient has verified its authenticity. This is because only the sender's public key will decrypt a digital signature encrypted with the sender's private key.

The program then creates a second message digest of the communication and compares the decrypted message digest with the digest the recipient created. If the two message digests match, the recipient knows that the communication has not been altered or tampered with, that is, the recipient has verified its integrity.

The effectiveness of the digital signature process depends upon the reliable association of a public-private key pair with an identified person. The discussion thus far has made one critical

---

[8] The Uniform Commercial Code (UCC) defines "signed" as "any symbol executed or adopted by a party with present intention to authenticate a writing." U.C.C. § 1-201 (39)(1991).

[9] Theoretically, it is possible for two people to randomly generate the same key, but the probability of this happening is staggeringly low *(i.e.,* one in untold quadrillions).

[10] *Digital Signature Guidelines* § 1.11.

assumption. That is, that the public-private key pair of the sender does, in fact, belong to the sender. Any assurance of authenticity would be worthless if the public key used to decrypt a digital signature belonged to an impostor and not the named sender.

Paper signatures usually have an intrinsic association with a particular person because they consist of that person's unique handwriting. However, public-private key pairs used to create digital signatures have no intrinsic association with anyone -- they are nothing more than large numbers. When a recipient obtains the public key of someone from whom he has received a digitally signed communication, how does he know that the public key does, in fact, belong to the purported sender? An impostor could have generated the public-private key pair under the purported sender's name.

The solution to this problem is to enlist a third party trusted by both the sender and recipient with performing the tasks necessary to associate an identified person with the key pair used to create the digital signature. Such a trusted third party is called a ***certification authority***.

2.2 CA's Role in Implementing Digital Signatures

A certification authority ("CA") is a trusted third party that ascertains the identity of a person, called a "subscriber," and certifies that the public key of a public-private key pair used to create digital signatures belongs to that person.[11] The certification process generally works in the following way. The subscriber:

1. generates his own public/private key pair using software on his computer;
2. visits the CA and produces proof of identity, such as a driver's license and passport or any other proof required by the CA; and
3. demonstrates that he holds the private key corresponding to the public key (without disclosing the private key).

These three steps in the certification process are likely to vary somewhat from CA to CA. For example, one CA may require a subscriber to appear in person before the CA as part of the second step of establishing the subscriber's identity. Another CA may be willing to rely on a third party, such as a notary, to establish the subscriber's identity.[12]

Once the certification authority has verified the association between an identified person and a public key, the certification authority then issues[13] a certificate. A certificate is a computer-based record that attests to the connection of a public key to an identified person or entity.[14] A certificate identifies the certification authority issuing it and the person (called a

---

[11] Utah Code Ann. § 46-3-103(5); *Digital Signature Guidelines* § 1.6.

[12] See, e.g., VeriSign, Inc., Notarial FAQ: Frequently Asked Questions, available at http://www.verisign.com/products/faqs/nota__faq.htm1 (relies on notaries to verify association of subscriber to a public key).

[13] Utah Code Ann. § 46-3-103(15)(1996); *Digital Signature Guidelines* § 1.16.

[14] Utah Code Ann. § 46-3-103(3); *Digital Signature Guidelines* § 1.5.

subscriber) identified with the public key. The certificate also contains the subscriber's public key and possibly other information, such as an expiration date for the public key.[15] To provide assurance as to the authenticity and integrity of the certificate the certification authority attaches its own digital signature to the certificate.

The certification authority then notifies the subscriber that the certificate has been issued so as to give the subscriber an opportunity to review the contents of the certificate before it is made public.[16] If the subscriber finds that the certificate is accurate, the subscriber may publish [17] the certificate, or direct the CA to do so, making it available to third parties who may wish to communicate with the subscriber. A certificate is published by being recorded in one or more repositories or circulated by any other means so as to make it accessible to all intended correspondents. A repository is an electronic database of certificates[18] -- the equivalent of a digital Yellow Pages. A repository is generally available online and may be maintained by the certification authority or by anyone providing repository services.[19] Repositories are generally accessible to anyone.

Repositories contain other important information as well. If a private key is compromised or lost, such as through loss of the medium on which it is stored or accidental deletion, it is generally necessary to suspend or revoke the corresponding certificate so that others will know not to rely on communications digitally signed with that key. This information is also posted in the repository.[20]

Once a certificate has been published, the subscriber may then append the certificate to any electronic communication. If the recipient wants to verify the connection between the sender and his public key, the recipient can look to the attached certificate for some assurance.

In a sense, the certificate is like a digital drivers license, which reliably identifies the subscriber online when used in combination with a digital signature. For example, if a subscriber were to digitally sign a purchase order, the party who receives that purchase order would rely on the subscriber's certificate to obtain the subscriber's public key and authenticate the digitally-signed purchase order. The party relying on a certificate in this manner is referred to as a *relying party.* After a CA issues a certificate, a potentially large numbers of persons may rely on that certificate ("relying parties") to ascertain the subscriber's public key.

A certificate that contains erroneous information is said to be *erroneously issued.* For example, suppose a malefactor tricks a CA by using a stolen drivers license belonging to the malefactors twin brother. The CA, reasonably believing that the malefactor is the person identified in the stolen drivers license, issues a certificate to the malefactor in the name of his

---

[15] Utah Code Ann. §§ 46-3-103(3); *Digital Signature Guidelines* § 1.5.

[16] *Digital Signature Guidelines* § 3.8(2)

[17] Utah Code Ann. § 46-3-103(29); *Digital Signature Guidelines* § 1.28.

[18] Utah Code Ann. § 46-3-103(29); *Digital Signature Guidelines* § 1.28.

[19] *See* Utah Code Ann. § 46-3-501.

[20] *See Digital Signature Guidelines* § 1.28 Comment 1.28.1.

twin. The malefactor may then use this erroneously issued certificate to impersonate the twin in online transactions. Parties who rely on the certificate may suffer financial losses when the twin repudiates the transaction. The impersonated twin may also suffer losses in defending claims by relying parties.

Even if a certificate is properly issued, if the subscriber losses or compromises his private key, a malefactor who comes into possession of that key could impersonate the subscriber by using the private key to digitally sign messages. Recipients of these messages who rely the subscriber's certificate would have no way of knowing that the subscriber's private key has fallen into the hands of an impostor. If the subscriber discovers that his key has been compromised, he may request the CA to "revoke" the certificate. Revocation is accomplished by the CA periodically publishing a list of revoked certificates called the "certificate revocation list" (CRL). To fully effectuate the revocation, it is necessary that the relying parties to check the CRL before relying upon a certificate.

2.3 Specific Functions of a CA

2.3.1 Overview

The functions of CA, generally discussed above, can be particularized into the following tasks, which are considered in more detail below:

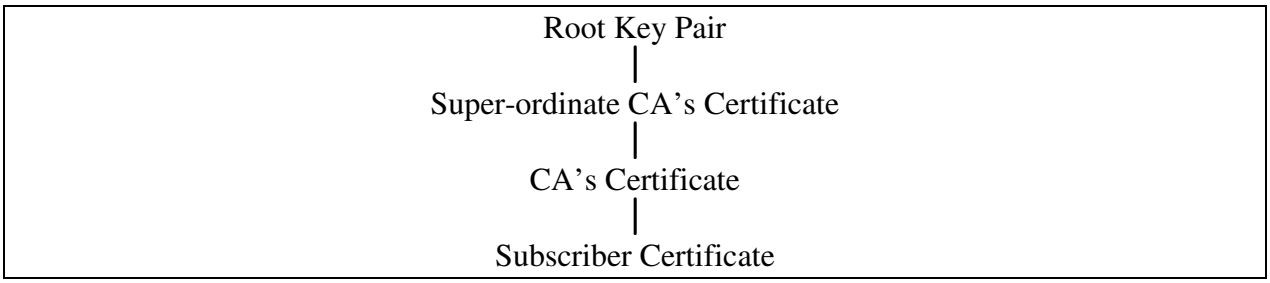
- Establish Signing Hierarchies
- Promulgate certificate policy and/or CPS
- Accept and Review Applications
- Name Subscribers
- Issue Certificates
- Maintain Repository
- Revoke and Suspend Certificates
- Ancillary Services

2.3.2 Establish Signing Hierarchies

One of the CA's first tasks is to create the signing hierarchy of keys and certificates that it will use in issuing digital certificates. At a minimum, the signing hierarchy consists of a signing key pair used by the CA to digitally sign the certificates that the CA issues to its subscribers. When a relying party receives a certificate issued by the CA, it uses the public key of the CA's signing key pair to verify that the certificate was in fact issued by the CA.

In verifying the authenticity of the certificate, the relying party may obtain the CA's public key from a trusted storage place (such as the relying party's own computer) or from yet another certificate that has been issued to the CA itself and which binds the identity of the CA to the CA's public key. The CA's certificate may be issued by the CA itself or by a super-ordinate (or root) CA such as a trade association CA or a government CA. The entity issuing the CA's certificate will use a separate signing key pair distinct from the signing key pair used to create the certificates issued by the CA.

Thus a relying party authenticating a certificate may rely upon a chain or "hierarchy" of certificates as illustrated by the table below. At the top of the hierarchy is the root key pair. The root key pair is used to issue a self-signed certificate root key, as there is no super-ordinate CA to certify the root.



2.3.3 Promulgate CPS

In an effort to limit its own liability and to help relying parties gauge the level of risk associated with its certificates, CAs may prepare and issue certification practice statements (CPS). A CPS contains information about the practices that the CA follows in its operations, details about the security of its system, and terms and conditions upon which its certificates are made available. These terms and conditions include suggested reliance limits and limitation of liability provisions applicable to subscribers and in some cases relying parties. For example, a CPS might specify that certificates are issued without any type of investigation and are suitable only for casual, non-commercial e-mail. Relying parties may refer to the CPS to assess the reliability of the certificates.

2.3.4 Accept and Review Applications

Once the CA establishes a signing hierarchy and promulgates a CPS, it typically must establish a process whereby candidate subscribers may apply to the CA for a certificate. Depending on the level of security the CA wishes to achieve, these applications may be in person, online, or via offline channels such as telephone or mail. If applications are to be accepted online, the CA will generally establish an appropriate vehicle for this such as a secure Web page. If applications are to be accepted in person, the CA will need to provide or contract for physical space (such as an office or storefront) where this may take place. When applications are accepted in person, an important step in the application process is the review of credentials proffered by the candidates. For example, if a CA intends to rely on a state-issued drivers license for verifying an applicant's identity, then the CA's personnel at the physical point of application will have the important duty of physically examining the drivers license to determine its authenticity (that is, that the person proffering the license is pictured on the license and that the name and address information of the license corresponds to the name and address information in the application).

Upon receipt of an application, the CA will process the application in accordance with the procedures specified in the CPS. The goal here is to verify that the identity of the applicant and to confirm that the applicant is in possession of the private key corresponding to the public key that will be listed in the certificate.

Depending on the level of security that the CA wishes to achieve this processing can range from the minimal (e.g., having a computer automatically issue the applied-for certificate) to extensive (e.g., conducting a detailed background check of the applicant). An emerging, intermediate procedure is to confirm that the information contained in the application matches information pertaining to the subscriber that is obtained from a third party provider, such as Dunn & Bradstreet.

2.3.5 Naming

It is important that subscribers of each certificate be uniquely named. To ensure this, the X.509 recommendation suggests use of a data construct called the *distinguished name,* which consists of fields such as country, organization, organization unit and common name. Use of these fields enables users with similar common names (example, Bob Jones and Bob Jones) to have distinct subject names because, presumably, the country, organization and organizational unit data will be different. To avoid confusion, the CA should ensure that each certificate it issues has a unique distinguished name.

In publishing a certificate, the CA is potentially making representation as to the correctness of each portion of the designated name. That is, the CA may be stating not merely that the subscriber is Bob Jones but that it is Bob Jones of IBM (the organization name). It has been suggested that CA's may wish to certify only a portion of the designated name of an individual subscriber and may wish to disclaim liability for correctness of the entire other fields such as common name and/or organization name.

2.3.6 Issue of Certificate

Upon approval of the application, the CA will physically generate a certificate and digitally sign it using the CA's private signing key. During this process, information contained in the subscriber's application may be transcribed into machine-readable format for inclusion in the certificate. Once the certificate is created and digitally signed, it is distributed to the subscriber by e-mail or other vehicles such as worldwide web page. A subscriber may indicate its acceptance of the certificate by an express message sent to the CA or by the subscriber's conduct (such as in downloading the certificate from a web page).

2.3.7 Maintain Repository

Once certificates have been issued and accepted by their subscribers, they are published by the CA in a repository, which is a database of certificates that is made accessible to all intended users. A repository may be generally available online.

2.3.8 Revoke and Suspend Certificates

During the operational period of a certificate, it may be necessary or appropriate to revoke or suspend the certificate. This may occur, for example, if the subscriber loses or otherwise compromises his or her private key, if the subscriber breaches his or her obligations to the CA, or if the information in the certificate otherwise becomes inaccurate. Revocation may performed by the CA's own initiative (subject to its agreement with subscribers) or may be requested by a subscriber.

The CA typically provides a robust channel for accepting revocation requests such as over the telephone or via e-mail. Upon receipt of a request, the CA determines whether a request is valid. Validation of a request may be performed by the requesting party using a shared secret (such as the subscriber's mother's maiden name) known only to the subscriber and the CA. Alternatively, a request for revocation may be authenticated by means of the subscriber digitally signing the request if the subscriber's private key is available.

Once the CA has received and authenticated a request for revocation, it effects the revocation by posting the revoked certificate to the CRL and/or issuing a revocation certificate. The CRL is periodically published by the CA to the repository. Alternatively, CRL's and/or revocation certificates may be distributed through other channels.

Once revoked, a certificate is no longer valid and cannot be reinstated. As an alternative to revocation, the CA may provide a suspension status, under which certificates may be temporarily disabled, such as when the named subscriber is on a prolonged vacation and will not be using the certificate.

2.3.9 Ancillary Services

CA's may provide ancillary services to subscribers and other persons including training, consulting and key escrow or key recovery services. We have assumed for purposes of our analysis that the CA will not be providing these types of ancillary services.

3. LIABILITY ANALYSIS -- PRELIMINARY CONSIDERATIONS

When analyzing the potential liability to which the CA may be exposed by virtue of its certification authority activities, it's helpful to consider two preliminary issues:

- To whom will the CA be potentially liable for damages?
- What activities of the CA could create liability exposure? (i.e., what types of things could go wrong?)

Following a discussion of these preliminary issues, the next sections will set forth a discussion of potential liabilities under the various legal theories.

3.1 Liability to Whom?

The potential liability of the CA for its activities will vary, in part, with respect to who could constitute a potential plaintiff. For purposes of the following discussion, we have focused on the following classes of potential plaintiffs who may have claims against the CA for damages:

- Subscribers - These are the persons identified in certificates issued by the CA
- Relying Parties - This is the class of persons that use and rely upon certificates issued by the CA. This will presumably include both businesses and consumers.
- Victims - This is a class of persons in whose names certificates are improperly issued by the CA (e.g. someone might fraudulently obtain a certificate in the name of Citicorp Bank when, in fact, they are not Citicorp. In such a case, Citicorp Bank would be the "victim" since the certificate could be used by the person perpetrating the fraud to enter into transactions in the name of Citicorp).

When analyzing the legal theories pursuant to which the CA may have liability exposure, it will be important (at least in some cases) to keep in mind who the injured party may be. For example, the ability of an injured party to recover in contract or in tort will vary depending upon whether such party is in contractual privity with the CA (such as a subscriber), or has no privity relationship with the CA (such as, perhaps, a relying party).

3.2 Activities Creating Liability Exposure

When operating as a certification authority, the entity will be engaged in a variety of activities that could expose it to liability.[21] Categorizing and understanding the things that can go wrong will be helpful in evaluating the scope of potential liability to which the CA may be exposed. For purposes of this analysis, we divide those activities into the following categories:

[21] For a general survey of CA activities creating liability exposure, see Michael S. Baum, U.S.Department of Commerce, *Federal Certification Authority Liability and Policy: Law and Policy of Certificate-Based Public Key and Digital Signatures* (June 1994)

3.2.1 Failure to Issue, or Delay in Issuing A Certificate.

As explained above, a CA typically issues certificates upon application by candidate subscribers. If an application meets the CA's criteria (presumably as set forth in the CPS), the CA may issue a certificate. Conceivably, an applicant might meet the criteria but nevertheless be rejected or delayed, either because the CA simply makes a mistake, because the CA's application facilities are unavailable by design or accident, or because the CA, for ulterior motives, wishes to delay or deny issuance of a certificate to the applicant. Applicants rejected or delayed under these circumstances may have claims against the CA.

Assuming a competitive market for CA services, there should be no real harm to an applicant if a CA were to refuse to issue a certificate, either by accident or design. However, in the absence of meaningful competition, a CA's refusal to issue a certificate or delay in issuing a certificate could be devastating where the rejected applicant is unable to engage in a particular business without the certificate. Even if competitive alternatives are available, one can envision transaction-specific losses where a certificate was requested in connection with a particular transaction, and as a result of delay or denial, the certificate was not available in time for the intended transaction, forcing to the applicant to forego the valuable transaction.

Likewise, if CA branded certificates become the *de facto* requirement for establishing trust for purposes of certain types of electronic transactions, the improper failure or refusal of the CA to issue a certificate to a qualified applicant may result in compensable business losses. In theory, this could occur notwithstanding the availability of alternative sources of certificates.

3.2.2 Erroneous Issuance to an Impostor

The principal function of a certificate is to bind an identity of the subscriber to a public key. Accordingly, the principal task of a CA is to verify, in conformance with its stated practices, that an applicant is the subscriber he or she purports to be, and that the applicant is in control of the private key corresponding to the public key listed in the certificate. It is expected that impostors may request certificates using fictitious identities or misappropriated identities of others. Ideally, the CA's procedures will prevent this from happening, but in some cases, certificates may be erroneously issued to impostors.

There are several circumstances that could lead to an erroneous issuance to an impostor. These include:

- Malfeasance. The CA's own employees or contractors conspire to issue erroneous certificates using the CA's signing key against improper applications by the impostor

- Misfeasance. The CA's employees or contractors negligently issue an erroneous certificate either by failing to properly perform the CA's stated validation procedures in reviewing the impostor's

application, or by using the CA signing key to create a certificate that has not been approved.

- Criminal Acts. A malefactor impersonates a subscriber using forged, but seemingly authentic, identification documents; despite careful and non-negligent adherence to its published policies, the CA issues a certificate to the impostor.

The consequences of an erroneous issuance to an impostor are potentially catastrophic. Relying parties who conduct on-line transactions with the impostor may rely on the incorrect data in the erroneously issued certificate and, as a result of that reliance, ship goods, transfer funds, extend credit, or undertake other transactions with the expectation that they are dealing with the impersonated party. When the fraud is discovered, the relying parties may have suffered substantial loses. For example, suppose an impostor obtains a certificate identifying it as the Bank of America. Using the certificate, the impostor provides a bogus letter of credit to a merchant, who, in reliance on that letter of credit, ships valuable goods overseas. When the merchant is unable to collect payment for the goods, it attempts to draw on its letter of credit, only to discover that the letter of credit is bogus and that it has no remedy against the purported bank. Of course, this type of fraud could be perpetrated on a much larger scale, involving multiple transactions and higher dollar volumes.

Notably, the impersonated party (Bank of America in the foregoing example) may suffer injury in two respects. First, it may be forced to expend resources in defending a claim by the duped merchant. Second, regardless of the outcome of the merchant's claim, the banks relationship with the merchant -- and perhaps its reputation with the public -- may be damaged by the incident.

In this situation, there are two injured parties: the relying who was defrauded by the erroneously issued certificate, (i.e. the merchant in the example above), and the person whose identity was impersonated in the erroneously issued certificate (i.e. the bank of the America in the example discussed above). Both will have claims against the CA.

3.2.3 False Repudiation

False repudiation describes a situation wherein a certificate is properly issued to a subscriber, and used by that subscriber in support of a transaction, but then subsequently falsely repudiated by the subscriber in the context of the transaction. That is, when the relying party in the transaction with the subscriber seeks to enforce performance by the subscriber, the subscriber denies that the certificate was issued to him -- i.e. the subscriber falsely claims that the certificate was erroneously issued to an impostor. While such a claim may be somewhat unlikely in the context of the community in which the certificates will be issued by the CA, should it occur it would likely trigger claims for recovery described in the preceding section. While the primary cause of such an occurrence would presumably be criminal or fraudulent conduct on the part of the subscriber (in falsely denying the certificate), other causes are also possible. This could include, for example, a misunderstanding or miscommunication within a subscriber bank that causes one person or department to repudiate a certificate that, unbeknown to it, was properly

obtained by another person or department within the same organization (perhaps by an individual who is no longer employed by the bank). This could stem, in part, from a lack of education and understanding as to the nature and functionality of public key cryptography digital signatures, and certificates.

3.2.4 CA Signing Hierarchy is Compromised

Certificates are issued by the CA using a signing hierarchy as described above. The most critical components of the signing hierarchy are the CA private signing key and the root key. The CA signing hierarchy will be compromised if either of these private keys are lost, disclosed to or used by unauthorized persons, or otherwise compromised.

The Signing Hierarchy may be compromised in at least three ways. First, the CA or its contractor could destroy or lose control of the key by mistake. For example, an CA employee could accidentally start a fire, destroying the data center that held the private key. Second, the CA's own employees and contractors may intentionally destroy or compromise the key for their own illegitimate purposes. Third, the key may be compromised by the criminal intrusion of a third party. For example, someone could attack the CA's data center and obtain the key through physical coercion or bribery of the CA's personnel. Fourth, the key may be compromised by a computational attack without any physical intrusion and with or without criminal motive. For example, a group of graduate students might develop an algorithm that allows someone to calculate the CA's private key using only the public key.

The consequences of a compromise of the signing hierarchy are potentially catastrophic in two ways. First, if either the private signing key or the root keys falls into the hands of a malefactor, such person can generate erroneous certificates at will and can use those certificates to impersonate real or fictitious subscribers to the detriment of relying parties. The potential for loss is even more substantial than in the case of a single isolated erroneous issuance.

Second, once the compromise is discovered, all certificates issued by the CA must be revoked, resulting in a potentially massive claim by the entire subscriber community for loss of use.

3.2.5 Subscriber Private Key is Compromised

Another potentially major problem, and one of the primary concerns with the use of digital signatures, is the situation wherein a subscriber's private key is compromised and improperly used by an impostor to defraud a relying party. In such a case, the "fault" for the compromise of the private key presumably lies with the subscriber, at least where the private key is generated by, and maintained under the sole and exclusive control of, the subscriber

3.2.6 Loss of Use of Repository or CRL

As part of its certification authority services, a CA often contemplates maintaining an online depository and CRL that will be accessible by relying parties for purposes of obtaining

copies of certificates and verifying their status as valid or revoked. Maintenance of this data base involves two basic risks:

- the risk that the repository or CRL may be inaccurate, thereby providing erroneous information upon which the recipient will rely to its detriment; and
- the risk that the repository or CRL will be unavailable (e.g. because of system failure), thereby interfering with the ability of subscribers and relying parties to complete transactions.

One case involves the publication of erroneous information. The other case involves the unavailability of information. In either situation, both subscribers and relying parties may suffer a loss as a result.

3.2.7 Failure to Suspend or Revoke

As discussed above, the use of a certificate is critical to the maintenance of digital signature infrastructure. Moreover, like the credit card system, it is critical that a mechanism be in place to determine in real time whether a particular certificate is valid, or whether it has been suspended or revoked. Whenever a private key is compromised, for example, revocation of the certificate is the primary mechanism by which a subscriber can protect itself from fraudulent transactions initiated by impostors who may have obtained a copy of their private key.

As a consequence, the speed with which the CA revokes or suspends a subscriber's certificate following a request from the subscriber is critical. The time interval between a subscriber's request to revoke a certificate and posting online of a CRL revoking that certificate may allow an impostor to enter into one or more fraudulent transactions. Thus, if the CA unreasonably delays in posting a revocation to the CRL, or fails to do so, both the subscriber and the defrauded relying party may suffer significant damages in reliance upon an allegedly valid certificate. In essence, the failure to post or delay in posting a revocation is like the publication of erroneous information by the CA on which others will rely.

3.2.8 Publication of Erroneous Information

When acting in its capacity as a certification authority, the CA is essentially engaged in the publication of three types of information: certificates, a repository of certificates, and a CRL. Subscribers will use this information to facilitate transactions with relying parties, and relying parties will use this information to determine the authenticity and integrity of the messages they receive from subscribers. Any errors of the publication of this information could have a significant adverse impact both upon the ability of subscribers to engage in electronic transactions and upon the ability of relying parties to accurately determine the authenticity and integrity of the electronic messages they receive.

3.2.9 Relationship with Third Party Outsourcer

In many cases, the CA desires to outsource a major portion of the responsibilities of the certification authority to a third party. Responsibilities that can be outsourced include manufacturing certificates, managing and maintaining certificates at a repository, revoking certificates, and updating a CRL identifying revoked certificates. As discussed in the foregoing sections, several key problems could occur with this process. To the extent that the source of these problems, or the ability to correct them, is not under the direct control of the CA, additional issues are raised. Also relevant is the extent to which the CA is liable for the conduct of the third party outsourcing entity should such problems occur.

3.2.10 Intellectual Property Infringement

Finally, it is possible that one or more aspects of the certification authority process could involve infringement of the intellectual property of third parties. Potentially involved are patent rights in the algorithms or processors employed, copyright rights in databases or documentation, trade secret rights and keys, processors, databases, or other aspects of the certification authority business, and finally, trademark rights relative to the naming used on certificates.

4. TORT LIABILITY - NEGLIGENT MISREPRESENTATION

4.1 General Definition

A tort is a violation of a duty imposed by law.[22] It is a civil wrong, other than a breach of contract, for which the law will provide a remedy in the form of an action for damages.[23] The aim of tort law is to protect the rights and privileges of persons against wrongful acts by others.[24] The law of torts is premised on the policy that a person who unreasonably interferes with the interest of another should be liable for the resulting injury and thus provides redress from wrongful acts that affect some legal interest of the complaining party.[25] Tort law attempts to allocate losses arising out of activity according to principles of fault,[26] and, consequently, in order to impose tort liability there must be fault.[27]

Negligence is perhaps the broadest category of tort liability imposed for harm caused to others. Negligence occurs when one fails to meet a recognized minimum standard of accountability to others for actions or activities that result in some damage to persons or property.[28]

When operating as a CA, an entity will primarily be in the business of providing information. Such information will take the form of certificates, a repository and a CRL. As such, the negligence-based cause of action most likely to be brought against the CA will be a claim for the tort of negligent misrepresentation.

The tort of negligent misrepresentation creates liability for communicating false information if the representation of a fact was intentionally made, but the defendant did not exercise reasonable care in determining its accuracy. The *Restatement (Second) of Torts* § 552, which provides the definition of negligent misrepresentation used by a majority of courts, states:

> § 552 Information Negligently Supplied for the Guidance of Others
>
> (1) One who, in the course of his business, profession or employment, or in any other transaction in which he has a pecuniary interest, supplies false information for the guidance of others in their business transactions, is subject to

---

[22] *Mills v. City of Overland Park*, 837 P.2d 370 (Kan. 1992); *City of Austin v. Houston Lighting & Power Co*., 844 S.W.2d 773 (Tex. Ct. App. 1992).

[23] *Haag v. Cuyahoga County*, 619 F. Supp. 262 (N.D. Ohio 1985), *affd,* 798 F.2d 1414 (6th Cir. 1986); *Steven K. v. Roni L.*, 164 Cal. Rptr. 618 (Cal. Ct. App. 2 1980)

[24] *Palco Linings, Inc. v. Pavex, Inc.*, 755 F. Supp. 1269 (M.D. Pa. 1990).

[25] *Gould v. Concord Hospital*, 493 A.2d 1193 (N.H 1985).

[26] *Nutt v. Loomis Hydraulic Testing Co., Inc.* 552 F.2d 1126 (5th Cir. 1977).

[27] *Album Graphics, Inc. v. Beatrice Foods Co.*, 408 N.E.2d 1041 (Ill. Ct. App. 1980).

[28] W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 30, at 164 (5th ed. 1984); RESTATEMENT (SECOND) OF TORTS § 282 (1965)?.

liability for pecuniary loss caused to them by their justifiable reliance upon the information, if he fails to exercise reasonable care or competence in obtaining or communicating the information.[29]

Thus negligent misrepresentation creates a duty for suppliers of information (such as a CA) to use "reasonable care or competence" in making representations to others (e.g., certificates, repositories, and CRLs), so as to prevent harm caused by justifiable reliance on that information. Most states accept negligent misrepresentation in their common law.[30]

This theory creates a duty to exercise reasonable care or competence to verify facts and creates liability for incorrect representations made without exercising reasonable care about the accuracy of the facts asserted.[31] It does not, however, make the information provider into a guarantor of the accuracy of the information. Under the *Restatement*, the information provider does not have liability for inaccurate or "false" information unless the provider failed to exercise reasonable care in obtaining or communicating the information. Thus, this does not create absolute liability, but rather a standard of care to which the information provider is held. A similar provision is included in proposed U.C.C. Article 2B.[32]

Negligence has four basic elements: (1) a legally-recognized duty to another person or class of persons; (2) breach of that duty by failing to meet the legally-recognized level of conduct (i.e., the "standard of care"); (3) the breach must actually cause, or be legally linked to, the cause of harm to a person or property; and (4) the complaining person must suffer compensible damages as a result of the activity.[33]

An analysis of the CA's liability for negligent misrepresentation as a certification authority therefore must address two basic issues:

(1) What is the legal duty, if any, owned by the CA; and

(2) To whom is such duty or obligation owed?

4.2 What is the Standard of Care Applicable to the CA?

A critical question for the CA is determining the standard of care against which its conduct as a certification authority will be measured and its potential liability to third parties determined. There are five possible standards of care that may apply: (1) a general standard of ordinary or reasonable care; (2) a professional standard of care; (3) a strict liability standard; (4)

---

[29] RESTATEMENT (SECOND) OF TORTS § 552(1) (1977).

[30] Nimmer, Information Law at ¶10.12 [2] at 10-43.

[31] See, e.g. *Computer Systems Engineering, Inc. v. Quantel Corp.,* 740 F.2d 59, 1st Cir. (1984). Nimmer, Information Law at ¶10.14 [1].

[32] U.C.C. Article 2B-404 (February, 1998 draft).

[33] W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 30, at 164 (5th ed. 1984); RESTATEMENT (SECOND) OF TORTS § 281.(1965)?

a statutorily mandated standard; and (5) possibly, a standard measured against criteria established by the CA itself.

4.2.1 General Standard of Reasonable Care

A general duty of care is imposed on all activities.[34] The duty of care most often required is that of "reasonable care," and that is the standard against which liability for negligent misrepresentation is most often measured.[35] Reasonable care, or ordinary care, may be defined simply as the degree of care that a person of ordinary prudence would exercise in the same or similar circumstances.[36] This is often referred to as the "reasonable person" standard. In other words, one is held to the same level of care and concern that the average, "reasonably prudent person" would exercise in a situation of similar circumstances.[37] It is a minimum, objective standard of conduct or risk assessment that society imposes on every member.[38] Viewed specifically from a business perspective, reasonable care means that degree of care that an ordinarily prudent and competent person engaged in the same line of business or endeavor would exercise under similar circumstances.[39]

In established industries where a common course of conduct has had time to emerge, assessing the general standard of care to which one will be held seldom presents any difficulty. Exercising reasonable care in those industries may involve little more than complying with the common practices of the industry, although such compliance will not always provide a safe harbor from negligence liability. In an industry as novel as that of the certification authority, however, appropriate standards of reasonable care have yet to be established.

The most prevailing factors in determining the applicable standard of care are the magnitude and foreseeability of the harm, the utility of the challenged conduct, the burden of guarding against the injury, and the relationship between the parties.[40] Thus, the standard of reasonable care with respect to any given activity is likely to be determined based upon a comparison of the magnitude of the risk involved to the social utility or value of the activity. As the magnitude and chances of harm from a given activity increase, the social utility of the activity must increase proportionately in order to justify the risk.[41] Viewed another way, the

---

[34] *See, e.g., Toone v. Adams,* 137 S.E.2d 132, 136 (N.C. 1964).

[35] RESTATEMENT (SECOND) OF TORTS, § 552(1).

[36] Black's Law Dictionary 1265 (6th ed. 1990) (citing *Pierce v. Horvath,* 233 N.E.2d 811, 815 (Ind. App. 1968)).

[37] *See Vaughn v. Menlove*, 132 Eng. Rep. 490 (1837); W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 32, at 174 (5th ed. 1984).

[38] W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 31, at 169 (5th ed. 1984).

[39] Black's Law Dictionary 1265 (6th ed. 1990) (citing *Warner v. Kiowa County Hospital Authority,* 551 P.2d 1179, 1188 (Okl. Ct. App. 1976)).

[40] *See Horak v. Biris,* 474 N.E.2d 13, 17 (Ill. App. Ct. 1985).

[41] *See* RESTATEMENT (SECOND) OF TORTS § 293 cmt. b (1965).

greater the risk of harm, the higher the degree of care necessary to constitute ordinary care.[42] The risk of harm involved includes economic loss as well as physical injury.[43]

These principles, although seemingly complex, may be explained quite simply. If an actor's conduct creates a foreseeable risk of harm, reasonable care requires the actor to undertake measures to prevent such harm so long as the cost of preventing that harm is less than the gravity of the harm multiplied by the probability that the harm will actually occur.[44]

Thus, the standard of care to be exercised in any particular case depends upon the circumstances of that case and on the extent of foreseeable danger.[45] As a consequence of the foregoing, it appears that the CA will need to consider the anticipated use of the certificates it issues, and ensure that its procedures are appropriate in light of those uses. For example, if CA certificates will be used only to identify subscriber bank Web sites that are provided primarily to advertise such banks and their services, the risk of loss resulting from an improper certificate may be relatively low. On the other hand, if CA certificates will be used to identify subscriber bank Web sites from which customers will disclose confidential information, issue fund transfer instructions, disclose PIN numbers, or otherwise conduct themselves in a manner that may result in more significant potential losses, the standard of care for issuing the certificates will be set at a much higher level. And if CA certificates will be used by subscriber banks to authenticate additional certificates issued by such banks as a CA, for a variety of purposes not yet known, the requirements may be much higher still.

Standard Applicable to Notaries. A Notary Public performs a function similar to that of a CA namely, identification. Thus it may be instructive to consider the standard of care imposed on notaries. Notaries are public officials authorized by their state governments to perform certain functions such as establishing the identity of persons brought before them, certifying their identity and signature on an official document such as an affidavit or deed, taking a person's acknowledgement that a signature previously made was made by them, or administering oaths or affirmations. Every state has a statute regulating the appointment and duties of notaries.

The standard to which notaries are held is one of reasonable care for the specific circumstances: "a notary must act as a reasonable notary would act under similar circumstances."[46] However, notaries are not insurers. They do not guarantee a person is who

---

[42] *Welsh Mfg. V. Pinkerton's, Inc.,* 474 A.2d 436, 440 (R.I. 1984), *later app.,* 494 A.2d 897 (R.I. 1985); *see also McMillan v. Michigan State Highway Commission,* 344 N.W.2d 26 (Mich. Ct. App. 1983), *aff'd in part, rev'd in part on other grounds,* 393 N.W.2d 332 (Mich. 1986) (duty required of actor is to conform to legal standard of reasonable conduct in light of apparent risk).

[43] *See People Express Airlines, Inc. v. Consolidated Rail Corp.,* 495 A.2d 107 (N.J. 1985).

[44] *See McMillan v. Michigan State Highway Commission,* 344 N.W.2d 26 (Mich. Ct. App. 1983), *aff'd in part, rev'd in part on other grounds,* 393 N.W.2d 332 (Mich. 1986).

[45] *DCR Inc. v. Peak Alarm Co.,* 663 P.2d 433, 435 (Utah 1983); *see also Glatt v. Feist,* 156 N.W.2d 819, 829 (N.D. 1968) (the amount or degree of diligence necessary to constitute ordinary care varies with facts and circumstances of each case).

[46] Michael L. Closen & R. Jason Richards, "Notaries Public—Lost in Cyberspace, or Key Business Professionals of the Future?", 15 J. Marshall J. Computer & Info. L. 703, 725 (Summer, 1997); *see also Naquin v. Robert*, 559 So.

they purport to be; they merely endeavor to take reasonable care to determine the identity of the person signing the document.[47] Reasonable care with respect to verifying identity differs from state to state. Some states have fairly stringent identification requirements[48] and specific procedures for verifying identity,[49] while others do not.[50]

Notaries are frequently held liable for negligence when they fail to follow common-sense procedures for verifying identity, such as by certifying a signature without seeing the person sign or having them acknowledge their signature in the notary's presence,[51] not asking to examine identification[52] or failing to ask a person if they are who they were introduced to be.[53] There is a general requirement that a person whose signature is being acknowledged or notarized appear before the notary in person.[54] Many states allow a notary to certify or take the acknowledgement

---

2d 18 (La. Ct. App. 1990) (reasonably skilled and prudent notary in same community); *Werner v. Werner*, 529 P.2d 370 (Wash. 1974) (notary must act reasonably); *In re Killingsworth*, 270 So. 2d 196 (La. Ct. App. 1972) (professional skill and diligence required of notary); *Transamerica Title Ins. Co. v. Green*, 89 Cal. Rptr. 915 (Cal. Ct. App. 1970) (notary must perform duties with honesty, integrity, diligence and skill); *Immerman v. Ostertag*, 199 A.2d 869 (N.J. Super. Ct. Law Div. 1964) (must exercise reasonable care in performance of notarial duties); *Levy v. Western Cas. & Sur. Co.*, 43 So.2d 291 (La. Ct. App. 1949) (notary must exercise same degree of precaution as reasonably prudent "business man").

[47] *See e.g.*, Alaska Stat. § 44.50.070; Ark. Code Ann § 21-14-111; Del. Code Ann. Tit. 29, §§ 4308, 4322; Fla. Stat Ann. § 117.05; Ga. Code Ann. § 45-17-8; Kan. Stat. Ann. § 53-503; *see also Myers v. Myers* 503 P.2d 59 (Wash. 1972); *see also City Consumer Serv., Inc. v. Metcalf*, 775 P.2d 1065 (Ariz. 1989) (en banc) (notary negligent in executing certification of acknowledgment when notary did not know signatory and failed to ask for identification or for acknowledgment of signature); *Browne v. Dolan*, 27 N.W. 795 (Iowa 1886).

[48] California, Florida, and Tennessee have a specific list of acceptable identification: State-issued driver's license or I.D. card; U.S. passport; foreign passport stamped by the Immigration and Naturalization Service; or a U.S. Military I.D. card. All must be issued within the last five years. "The I.D. Puzzle," The National Notary Magazine, September 1996, p. 9 (in Michael L. Closen, et al., Notary Law & Practice: Cases & Materials 180-81 (1997)).

[49] For example, as of 1996, California has a new program requiring a notary to obtain a right thumbprint of a person signing in-state any deed involving real property, whether located in or out of the state. "State's Notaries Get Ready For Unique Print Statute," Notary Bulletin, December, 1995, p. 1 (n Michael L. Closen, et al., Notary Law & Practice: Cases & Materials 180-81 (1997)).

[50] In some states the only official statement on what constitutes acceptable procedures comes from pamphlets published by the Secretary of State's office, without much official guidance. For example, Indiana's Notary Public Pamphlet states that "a driver's license or credit card is usually good identification." "The I.D. Puzzle," The National Notary Magazine, September 1996, p. 9 (in Michael L. Closen, et al., notary law & practice: cases & materials 180-81 (1997)). Other states offer similarly limited guidance.

[51] *See, e.g., Biakanja v. Irving*, 320 P.2d 16, 17-18 (Cal. 1958) (Notary failed to have will properly attested, certified signatures made outside his presence).

[52] *Immerman v. Ostertag*, 199 A.2d 869, 871 (N.J. 1964) (Notary watched persons sign document, but never requested identification).

[53] *See, e.g., City Consumer Services, Inc. v. Metcalf*, 775 P.2d 1065 (Ariz. 1989) (Notary held liable for negligence in certifying signature of woman introduced as wife of a man known to him, but who was not).

[54] MICHAEL S. BAUM & HENRY H. PERRITT, JR., ELECTRONIC CONTRACTING, PUBLISHING, AND EDI LAW 218 (1991); *see also* National Conference of the Commissioners on Uniform State Laws, Uniform Law on Notarial Acts § 2, cmt. (1983). As these commentators point out, such a requirement would be difficult to apply to CA functions since "[t]he benefits of electronic transactions are premised on their speed and efficiency. Physically traveling to a notary and undertaking conventional notarial ceremonies within an electronic environment is impractical."

of a signature on the basis of their own personal knowledge of a person, or their identification by same one who is personally known to the notary.[55] Notaries in many states have considerable latitude in determining a person's identity, particularly in states without specific statutory identification requirements: "With respect to the identities of signers, the law requires nothing more of the notary than the use of reasonable care to satisfy himself . . . that the signers are the persons they purport to be."[56] However, the standard of reasonable care may create a minimum standard, and to go below that may subject a notary to liability: "mere conformity with custom is not necessarily to be equated with the exercise of reasonable care, because the custom itself may not meet the 'reasonable man' standard."[57] The practices of other notaries are probative, but not conclusive evidence of what constitutes reasonable procedures.[58] Where notaries are themselves the victims of fraud or intentional deception, they will not be held liable unless their conduct was itself negligent, although they may have the burden of proving they took reasonable care in identifying the signatory.[59]

4.2.2 **Professional Standard of** Care

The standard of care becomes heightened for those who are considered to be professionals.[60] They are held to a standard of knowledge and skill equivalent to the average member of their profession.[61] Even among professionals, specialists in a particular subject will be held to the standard reasonable for one with the special information or skills they possess.[62] Thus, for example, a doctor will be held to a general "reasonable care" standard for drivers if he is involved in a car accident, but to the professional standard of care for a doctor if he treats someone hurt in the accident, and perhaps to a higher standard as a specialist if he is in fact a trauma surgeon who regularly treats accident victims.

Professional liability for negligence is applicable only to those persons deemed to be a professional. Courts traditionally limit professional liability to those who fall into particular professions. Doctors, attorneys, and accountants are the most commonly recognized, but the

---

MICHAEL S. BAUM & HENRY H. PERRITT, JR., ELECTRONIC CONTRACTING, PUBLISHING, AND EDI LAW 218 n.266 (1991).

[55] *See* Michael L. Closen & G. Grant Dixon, *Notaries Public From the Time of the Roman Empire to the United States Today, and Tomorrow*, 68 N.D. L. Rev. 873, 883-884 (1992); *see also, e.g.*, 5 ILL. COMP. STAT. ANN. 312/6-102.

[56] *Immerman v. Ostertag*, 199 A.2d 869, 873 (N.J. 1964)

[57] *Myers v. Myers,* 503 P.2d 59, 63 (Wash. 1972).

[58] *Myers v. Myers,* 503 P.2d 59, 62-63 (Wash. 1972).

[59] Michael L. Closen & R. Jason Richards, "Notaries Public—Lost in Cyberspace, or Key Business Professionals of the Future?" 15 J. Marshall J. Computer & Info. L. 703, 727 (Summer, 1997).

[60] W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 32, at 185 (5th ed. 1984).

[61] W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 32, at 185 (5th ed. 1984); *see also* RESTATEMENT (SECOND) OF TORTS § 299A.

[62] W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 32, at 175 (5th ed. 1984).

courts have recognized many other professions as well.[63] Professionals are persons deemed to possess specialized knowledge and skills beyond that of ordinary laypersons, usually licensed by an official body, and held to certain standards of conduct, such that people place them in special trust beyond the standards of the marketplace, and the courts therefore hold them to a higher standard of care.[64] One court has offered the following definition:

> A profession is not a business. It is distinguished by the requirements of extensive formal training and learning, admission to practice by a qualifying licensure, a code of ethics imposing standards qualitatively and extensively beyond those that prevail or are tolerated in the marketplace, a system for discipline of its members for violation of the code of ethics, a duty to subordinate financial reward to social responsibility, and, notably, an obligation on its members, even in non-professional matters, to conduct themselves as members of a learned, disciplined, and honorable occupation.[65]

Professionals must have a minimum amount of special knowledge and skills necessary to act as a member of the profession, and have a duty to act as a reasonable member of the profession would in a given circumstance.[66] Professionals who hold them out as specialists even within the profession, such as a doctor who practices as an obstetrician, are held to an even higher standard of care reasonable for practitioners of that specialty.[67]

Under this definition, not everyone with specialized skills is a professional; something more is required.[68] For example, computer professionals have not been accepted as professionals by the courts[69]; although they have specialized skills, they are not subject to recognized educational standards, a code of conduct, or licensing or disciplinary bodies.[70] Likewise, it does not appear that certification authorities will be held to a professional liability standard at this early stage: "there are no usages of trade that might help define the standard of care that one might expect of a CA . . . no licensing or professional bodies whose standards could serve as the

---

[63] Architects, Engineers, Dentists, Pharmacists, Psychiatrists, Veterinarians, Title and Abstracters have all been recognized as professionals. *See* W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 32, at 185-86 (5th ed. 1984).

[64] *Hosp. Computer Systems v. Staten Island Hosp.*, 788 F. Supp. 1351, 1361 (D. N.J. 1992).

[65] *In re Estate of Freeman*, 311 N.E.2d 480, 483 (N.Y. 1974).

[66] W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 32, at 187 (5th ed. 1984).

[67] W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 32, at 187 (5th ed. 1984).

[68] *See Reich v. City of Reading*, 284 A.2d 315, 319 (Pa. Commw. Ct. 1971) ("the word 'profession' connotes something more than mere skill in the performance of a task.") (quoting *Howarth v. Gilman*, 73 A.2d 655, 658 (Pa. 1950)).

[69] *See generally*, Michael Rustad & Lori E. Eisenschmidt, "The Commercial Law of Internet Security," 10 High Tec. L. J. 213, 243-252 (1995) (discussing potential professional liability for Internet security professionals).

[70] *Hosp. Computer Systems v. Staten Island Hosp.*, 788 F. Supp. 1351, 1361 (D. N.J. 1992) (computer vendor not liable for malpractice because not member of a recognized profession); *see also Invacare Corp. v. Sperry Corp.*, 612 F. Supp. 448, 453-54 (N.D. Ohio 1984) (no liability for computer malpractice); *Chatlos Sys., Inc. v. National Cash Register Corp.*, 479 F. Supp. 738 (D. N.J. 1979) (rejecting concept of computer malpractice in sales and service of computer equipment).

basis for a legal norm."[71] However, at least one commentator argues that the recognition of CAs as professionals may not be far down the road as statutes are enacted, many of which draw on the American Bar Association *Digital Signature Guidelines*, to provide a basis for holding CAs to standardized levels of training, conduct, and care.[72] Moreover, as more states seek to license CAs, such as Utah, Washington, Minnesota, Florida, and Mississippi, courts may eventually be willing to impose professional negligence standards.

Additionally, the fact that CAs by their nature will be parties with specialized skills in whom laypersons place trust beyond that of the normal marketplace may give them status as professionals.[73] And even if CAs are not considered professionals, they may have a higher duty of care given their specialized skills.[74]

4.2.3 Strict Liability

Unlike liability in negligence, which requires a finding of fault, in certain cases, courts will impose "strict liability" for harm caused regardless of fault. Strict liability is a judge-made policy based rule that no finding of fault by the maker of a product is required to hold the maker liable for any harm caused to another person by the product; they are held to be liable simply for placing a defective product on the market. No showing of negligence, breach of warranty, or intentional conduct is required.[75] The producer of the product is liable to any person whose injuries were causally linked to the product defect. Responsibility is assigned directly to the manufacturer because it is in the best position to prevent any such defects from injuring people.

To date, strict products liability generally has been applied only to products (not to services), and only when the defect in the product results in physical harm to a person or property.[76] The requirement of physical harm makes it unlikely that a CA would will face strict liability, even if a certificate is determined to be a product. However, it should be noted that there was support from several countries participating in the UNCITRAL Working Group on Electronic Commerce for a rule that would impose strict liability on a certification authority for improper identification in a certificate. At the February 1997 UNCITRAL meeting, a tentative compromise solution was to impose a so-called "rebuttable strict liability" standard on CAs.[77]

---

[71] A. Michael Froomkin, "The Essential Role of the Trusted Third Parties in Electronic Commerce," 75 Or. L. Rev. 49, 92 (Spring, 1996).

[72] A. Michael Froomkin, "The Essential Role of the Trusted Third Parties in Electronic Commerce," 75 Or. L. Rev. 49, 92 n.152 (Spring, 1996) (Positing that the CA Digital Signature Guidelines may eventually provide the standards for recognition of certification authorities as professionals).

[73] *Hosp. Computer Systems v. Staten Island Hosp.*, 788 F. Supp. 1351, 1361 (D. N.J. 1992) ("Professionals may be sued for malpractice because the higher standards of care imposed on them by their profession and by state licensing requirements engenders trust in them by clients that is not the norm of the marketplace.").

[74] W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 32, at 185 (5th ed. 1984).

[75] *Greenman v. Yuba Power Products, Inc.* 377 P.2d 897 (Cal. 1963).

[76] W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 98, at 92-94 (5th ed. 1984); *Greenman v. Yuba Power Products, Inc.* 377 P.2d 897 (Cal. 1963).

[77] See, United Nations Commission on International Trade Law, "Report of the Working Group on Electronic Commerce on the Work of its Thirty-First Session," A/CN.9/437 (March 12, 1997) at Pars. 56-59.

That is, the law would presume that a CA is liable for an improper identification in a certificate, but that presumption could be rebutted by a showing that the certification authority "had done its best efforts to avoid the error," and that notwithstanding such procedures a mis-identification occurred. The U.S. has expressed its opposition to this liability position, and it appears that support for this position was further eroded at the January 1998 UNCITRAL meeting. Nonetheless, it was raised, and it should be recognized as a potential source of liability, especially if the CA proposes to do business outside the United States.

4.2.4 Statutorily-Defined Standards of Care

The standard of conduct to which an actor will be held in some instances may be prescribed by statute. A statute may, for example, set forth particular acts that an actor is required to undertake in connection with certain activities, or on the other hand it may prohibit engaging in certain acts. When an actor fails to comply with such prescribed standards, this may serve as a basis for finding negligence if the other elements of negligence exist.

In connection with a CA's activities, some states already have established statutory standards of care to which a licensed CA will be held. In Utah, for example, the Utah Digital Signature Act (the "Utah Act")[78] imposes upon a licensed CA certain specific duties and obligations in connection with, among other things, issuing and revoking certificates. Although the Utah Act and other similar state statutes generally apply only to CAs licensed in that respective state, such statutes may nevertheless serve as a model for measuring the reasonableness of a CA's conduct in states where such statutes do not yet exist. Thus any CA would be well advised to take these and other statutory standards of care under consideration when establishing the procedures to which it will adhere in connection with offering CA services.

Because Utah was the first comprehensive digital signature act to be enacted, and because it has since served as a model for various other enacted and proposed state digital signature statutes,[79] it is worth examining some of the most basic duties it imposes upon CAs licensed in Utah.

Issuing Certificates. The Utah Act imposes various duties upon a licensed CA in connection with the issuance of certificates. Specifically, the Utah Act requires that CA may issue a certificate only after it has confirmed that:[80]

(i) the prospective subscriber is the person to be listed in the certificate to be issued;

---

[78] Utah Code Ann. §§ 46-3-101 to -504 ([1995 and Supp. 1996]). *See also* Utah Admin. R. 154-10-100 to -501 (1997) (regulations pertaining thereto).

[79] As of February, 1998 two states have enacted digital signature statutes modeled after the Utah Act. They are Washington (Wash. Rev. Code Ann. §§ 19.34.010 to .903) and Minnesota (Minn. Stat. Ann. §§ 325K.001 to .26). Numerous other states are currently considering adopting digital signature statutes substantially similar to that of Utah. They include: Hawaii (1997 Senate Bill 961); Michigan (1997 Senate Bill 204); Missouri (1998 House Bill 1126 and 1998 Senate Bill 708); New York (1997 Senate Bill 2238 and 1997 Assembly Bill 6183); Rhode Island (1997 Senate Bill 612); and Vermont (1997 Senate Bill 206 and 1997 House Bill 60).

[80] Utah Code Ann. §46-3-302

(ii) if the prospective subscriber is acting through one or more agents, the subscriber authorized the agent or agents to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;

(iii) the information in the certificate to be issued is accurate after due diligence;

(iv) the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(v) the prospective subscriber holds a private key capable of creating a digital signature; and

(vi) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber.

Revoking Certificates. The Utah Act also sets forth certain statutory requirements with respect to which a licensed CA must comply in connection with the revocation of certificates.[81] These include a requirement that the CA "confirm that the person requesting revocation is that subscriber, or is an agent of that subscriber with authority to request the revocation."

General Requirements for CAs. Aside from imposing certain specific duties in connection with the issuance and revocation of certificates, CAs licensed in Utah are also subject to various general duties.[82] For example, a licensed CA is required to:

(1) use only a trustworthy system to issue, suspend, or revoke a certificate, to publish or give notice of the issuance, suspension, or revocation of a certificate, or to create a private key.

(2) disclose any material certification practice statement, and any fact material to either the reliability of a certificate which it has issued or its ability to perform its services.

The above examples are just some of the statutory requirements that collectively establish the standard of care to which a CA licensed in Utah will be held. CAs not licensed in Utah may be well advised to take under consideration these and other regulatory requirements pertaining to CAs because courts in other states may look to them as a source for measuring a CA's standard of conduct.

4.2.5 Self-Defined Standards of Care

A critical question is whether the CA can, itself, establish the standard against which its conduct will be judged. In other words, can the CA, through the use of a certificate policy,

[81] Utah Code Ann. §46-3-307

[82] Utah Code Ann. §46-3-301

certification practice statement, or other form of notice, outline the procedures, undertakings, duties, obligations, and responsibilities that it is willing to undertake, and (provided it lives up to those standards), be assured that any losses resulting from reliance on erroneously issued certificates, repositories, or CRLs will result in liability only if they were caused by a failure to comply with the standards that the CA set for itself? Or, alternatively, does the law on behalf of the CA impose some minimum set of standards (e.g., reasonable care), which, from a policy perspective, will always apply to the CA's activities?

This is a difficult question and one to which there is not a readily apparent answer. Virtually all certification authority activity to date is premised on the proposition that the CA can, through a certificate policy, certification practice statement, or other similar device, define the nature of the product or service it is providing and, thereby, set the standard against which its performance will be judged.[83]

As a general rule, however, the conduct of a person is not to be judged by his own standard.[84] Whether a certain course of conduct is negligent is ordinarily determined by the standard fixed by law without regard to any private rules of a party.[85] In other words, it appears that questions of negligence must ordinarily be determined with reference to standards of conduct prescribed by law.[86]

(a) The Relevance of Industry Custom.

This conclusion is also reflected in the use of industry custom to determine the applicable standard of care. It is a well-established principle of tort law that industry custom is a relevant, but by no means conclusive consideration in determining the standard of care against which an actor's conduct will be measured.[87] The reason for limiting an actor's reliance on industry custom is that the custom itself may be negligent. Moreover, "if the only test is to be what has always been done, no one will ever have any great incentive to make any progress in the direction of safety."[88] As the leading authorities on torts have put it:

---

[83] *See, e.g.*, American Bar Association *Digital Signature Guidelines*, Section 1.8 ("certification practice statement"), and Comment 1.8.2 (noting that "the duties a certification authority owes to a relying person are generally based on the certification authority's representations, which may include a certification practice statement."), and Comment 1.83 (noting that "whether a certification practice statement is binding on a relying person . . . depends on whether the relying person has knowlede or notice of the Certification Practice Statement.").

[84] *South Atlantic S.S. Co. of Delaware v. Munkacsy*, 187 A.600, 604; *Dixon v. General Grocery Co*., 293 S.W.2d 415, 421; CJS *Negligence*, Section 1(4).

[85] *Snider v. Callahan*, 250 F.Supp 1022 (W.D. Mo. 1966); *Fonda v. St. Paul City Railway Co*., 74 N.W. 166 (Minn. 1898); *Fries v. Goldsby*, 80 N.W.2d 171 (Neb. 1956).

[86] *U.S. v. Ohio Barge Lines, Inc.,* 607 F.2d 624 (3rd Cir. 1979).

[87] *See Darling v. Charleston Community Memorial Hospital,* 211 N.E.2d 253 (Ill. 1965), *cert. denied,* 383 U.S. 946 (1966); *see also Texas & Pacific Railway Co. v. Behymer,* 189 U.S. 468, 470 (per Just Oliver Wendell Holmes) ("What usually is done may be evidence of what ought to be done, but what ought to be done is fixed by a standard of reasonable prudence, whether it is usually complied with or not"). See also, W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 33, at 193 (5th ed. 1984).

[88] RESTATEMENT (SECOND) OF TORTS § 295A cmt. c (1965).

> customs and usages themselves are many and various; some are the result of careful thought and decision, while others arise from the kind of inadvertance, carelessness, indifference, cost-paring and corner-cutting that normally is associated with negligence . . . [But] Even an entire industry, by adopting such careless methods to save time, effort or money, cannot be permitted to set its own uncontrolled standard.[89]

This principle may have been best highlighted in the seminal case of *The T.J. Hooper*[90] In that case, Judge Learned Hand rejected the defense of custom as a "safe harbor" from negligence where two barges and their cargo might not have been lost at sea had the boats towing them been equipped with weather radios. It was not customary in the industry at that time to install such radios in tugboats. Nevertheless, Judge Hand stated:

> Indeed in most cases reasonable prudence is in fact common prudence, but strictly it is never its measure; a whole [industry] may have unduly lagged in the adoption of new and available devices. [An industry] never may set its own tests, however persuasive be its usages. Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.[91]

Embedded in this principle that the industry itself cannot be permitted to set its own uncontrolled standards is the concept that some implicit minimum standard of care applies with respect to any given activity. Thus it seems logical that the standards established by the first actors in a novel industry will not go unchecked. If challenged, such standards most likely will only be deemed reasonable to the extent that they meet or exceed the minimum standards of reasonable care imposed by the courts, which are commensurate with the magnitude of the risks involved.

(b) Savings Bank Cases.

One early line of cases that highlights the above concepts and that seems particularly relevant to the situation at hand are those cases dealing with the liability of savings banks (and sometimes commercial banks) for improperly allowing persons in possession of a depositor's lost or stolen passbook or savings account card to withdraw from the account.

Historically a passbook served two functions: (1) it provided the account holder with a record of deposits and withdrawals; and (2) it provided some evidence of ownership of the account since presentation of the passbook was generally necessary to withdraw money from the account. In an attempt to limit their exposure to liability for unauthorized withdrawals by imposters, many savings banks would adopt bylaws or rules purportedly authorizing them to allow anyone in possession of the passbook to withdraw from the account, unless notice of the lost passbook was given to the bank prior to the making of the payment. These provisions would

---

[89] W. PAGE KEETON, ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 33, at 194 (5th ed. 1984).

[90] *In re Eastern Transp. Co. v. Northern Barge Corp.*, 60 F.2d 737 (2d Cir. 1932) (The T.J. Hooper case).

[91] *In re Eastern Transp. Co. v. Northern Barge Corp.*, 60 F.2d 737, 740 (2d Cir. 1932) (The T.J. Hooper case).

also be incorporated into the depositor's account agreement (and sometimes would even be printed inside the passbook itself) and thus, when assented to by depositors, formed a part of the contract of deposit.

Although such exculpatory provisions were generally upheld, in most cases the liability of the bank for making payments upon the presentation of a lost or stolen passbook or savings account card nevertheless hinged upon whether the bank had exercised reasonable care in making the payment in light of the particular facts and circumstances of each case. If the bank was found to have failed to exercise reasonable care given a specific set of circumstances, then it was liable in negligence regardless of its compliance with its own standards and industry custom. For example, in *First National Bank v. Stephens*, the court held that such a rule did not operate to discharge the bank for its own negligence because the bank had a duty that was founded upon public policy to exercise reasonable care and diligence in making payments from a savings account.[92] Thus despite the industry's attempt to limit its liability by defining its own standard of conduct, and despite the fact that such a standard was not deemed to be unreasonable *per se,* the banks were still held to some sort of minimum standard of reasonable care.

Likewise, these cases illustrate the fact that what constitutes reasonable care generally requires an examination of the relevant facts and circumstances of each case. In some cases, for example, reasonable care may require an actor to adopt new means of precaution as they become available. In other cases, failure to do something in one case that would not be required in another could constitute negligence.

In one early case a bank was found negligent for payments made to an impostor for not having the means available to make a signature comparison. The court held that the bank had not exercised reasonable care by virtue failing to institute a signature card system for comparing the presenter's signature with that of the true account holder.[93] Significant to the court's decision was the fact that the bank could have personally known only a small percentage of its over 12,000 depositors and thus sole reliance on the possession of a passbook was not sufficient to reduce the risk of loss. The court reasoned that a simple and inexpensive means of aiding identification could have been established by creating a central file containing account holder's signatures against which the signatures on withdrawal slips could be compared. Failure to do so in this case constituted negligence.[94] In *Rosen v. State Bank*[95] the court held that failure on behalf of a bank to personally inquire about the validity of the withdrawal at the account holder's place of business, which was in close proximity to the bank, constituted negligence where bank

---

[92] 184 S.E.2d 484 (Ga. Ct. App. 1971); *see also Kalb v. Chemical Bank New York Trust Co.,* 309 N.Y.S.2d 502 (N.Y. City Civ. Ct. 1969), *rev'd on other grounds,* 316 N.Y.S.2d 381 (N.Y. Sup. App. 1970) (fact that bank has printed in passbooks rule that payment shall be made to person presenting passbook does not relieve bank of general duty to exercise care in making payments because public policy will not allow bank to strip itself of responsibility by contract as to enable it to safely pay, intentionally or heedlessly, to one who has come into possession of passbook fraudulently or criminally); *Watts v. American Security & Trust Co.,* 47 A.2d 100 (D.C. Mun. Ct. App. 1946) (question of what constitutes reasonable care depends upon circumstances of each case).

[93] *Ladd v. Augusta Savings Bank,* 52 A. 1012 (Me. 1902).

[94] *Ladd v. Augusta Savings Bank,* 52 A. 1012 (Me. 1902).

[95] *Rosen v. State Bank*, 65 N.Y.S. 666 (N.Y. City Ct. 1900).

officers noticed that the mark made by the presenter was not identical to that contained in the bank's signature book.[96] The court reasoned that the bank's close proximity to the depositor's place of business presented a opportunity which, if acted upon, would have prevented the loss.[97]

In a more recent case it was held that the failure to ask test questions, such as mother's maiden name, in addition to presentment of a passbook might be evidence of negligence in a particular transaction.[98]

4.3. To Whom Does the CA Owe a Duty?

4.3.1 Approaches to Determine to Whom a Duty is Owed

Understanding the scope of liability for "information negligence" requires identifying to whom the CA owes a duty of care.[99] If a CA is sued for negligent misrepresentation based on a false or erroneous certificate, repository, or CRL, the first question will be whether the CA owed a duty of care to that particular person. CAs potentially have duties under tort to three groups of people: (1) subscribers, (2) parties relying on certificates, whether known or unknown ("Relying Parties"), and (3) third party victims of fraud.

Here, one can productively describe a continuum that begins with duties owed to persons with whom the CA enters into a direct contract (e.g., subscribers) and eventually extends to any third party who receives and relies on the information (e.g., the certificate) provided. Just how far the continuum extends entails a "privity" question and a unique problem in information law.

The nature of the relationship between the information provider and the party whose reliance resulted in loss is often critical in determining liability for misinformation. For example, a lawyer or accountant owes a far different duty in her relationship with a client than in her relationship with remote parties with whom no contract exists.[100] Duties of care to provide accurate information differ significantly in that comparison, with the result often being to limit liability of the professional to cases involving clients or directly intended recipients of the information. Similarly, a newspaper owes different obligations to its readers, whose relationship is defined by the small fee to purchase a copy, than a stockbroker owes to his clients.[101]

---

[96] *Rosen v. State Bank*, 65 N.Y.S. 666 (N.Y. City Ct. 1900).

[97] *Rosen v. State Bank*, 65 N.Y.S. 666 (N.Y. City Ct. 1900).

[98] *See Novak v. Greater New York Savings Bank,* 282 N.E.2d 285 (N.Y. 1972).

[99] The CA, operating as a CA, potentially owes a duty to three groups of people: (1) subscribers (i.e., the persons to whom certificates are issued), (2) parties relying on certificates, repositories, and CRLs issued or maintained by the CA ("relying parties"), and (3) third party victims of fraud.

[100] See, e.g., *Bily v. Arthur Young & Co.,* 834 P.2d 745, 3 Cal. 4th, 370 (1992).

[101] NIMMER, INFORMATION LAW at ¶10.13 [2].

In addressing issues of the liability of information providers to third parties, courts generally find that a duty is owed to one of the following three classes of potential plaintiffs (from most expansive to most restrictive):[102]

(1) **Persons Foreseeable** -- under this standard, the CA is liable to any person for whom reliance on the false representations was reasonably foreseeable. The foreseeability standard creates the broadest liability applicable to information.

(2) **Persons Intended or Known -- Restatement Approach** -- under this standard, the liability of the CA is limited to losses suffered (a) by persons for whose benefit and guidance the information provider intends to supply the information or knows that the recipient intends to supply it; (b) through reliance upon it in a transaction that he intends the information to influence, or knows that the recipient so intends, or in a substantially similar transaction (the Restatement approach). This supplants general foreseeability with a standard centered on the information provider's intent or knowledge with respect to particular individuals and to the type of transaction in which the information will be used. The *Restatement* standard has been widely adopted.[103] This rule subjects the negligent supplier of misinformation to liability only as to those persons for whose benefit and guidance it was supplied.

Under this theory it is not necessary that the maker should have any particular person in mind as the intended, or even the probable, recipient of the information. In other words, it is not required that the person who is to become the plaintiff be identified or known to the defendant as an individual when the information is supplied. It is enough that the maker of the representation intends it to reach and influence either a particular person or persons, known to him, or a group or class of persons distinct from the much larger class who might reasonably be expected to have access to the information and to take some action in reliance upon it. It is enough, likewise, that the maker of the representation knows that the recipient intends to transmit the information to a similar person, persons or group. It is sufficient, in other words, insofar as the plaintiff's identity is concerned, that the maker supplies the information for repetition to a certain group or class of persons and that the plaintiff proves to be one of them, even though the maker never had heard of him by name when the information was given. It is not enough that the maker merely knows of the ever-present possibility of repetition to anyone, and the possibility of action and reliance upon it, on the part of anyone to whom it may be repeated.[104]

> **Illustration.** A, having lots for sale, negligently supplies misinformation concerning the lots to a real estate board for the purpose of having the information incorporated in the board's multiple listing of available lots, which is distributed by the board to approximately 1,000 prospective purchasers of land each month. The listing is sent by the board to B, and in reliance upon the misinformation B purchases one of A's lots and in consequence suffers pecuniary loss. A is subject to liability to B.[105]

---

[102] Nimmer, Information Law at ¶10.15 [1][b] at 10.61.

[103] Nimmer, Information Law at ¶10.15 [1][b] at 10.61.

[104] RESTATEMENT (SECOND) OF TORTS, § 552 comment h.

[105] RESTATEMENT (SECOND) OF TORTS, § 552, illustration 4.

(3) **Persons in Privity/Near Privity** -- An alternative approach is to limit negligence theory to a duty owed solely to the client. This emphasizes concepts of privity of contract or, at least, "near" privity by requiring conduct specifically linking the information provider to the injured or relying party. Some states adopt this approach as a matter of common law while others adopt statutory applications of it.

4.3.2 Applications to Specific Information Providers

Application of these various approaches can be seen in a variety of cases that may be analogous to the information providing function of a CA.

(a) Accountant's Liability

Accountant practice has aspects particularly analogous to the role of the CA in a transaction. Accountants most often face suits by third parties based on negligent misrepresentation for their independent audits of company finances.[106] Courts are divided as to how these cases should be treated using the three approaches identified above.

(1) Privity/Near Privity

The Privity/Near Privity approach is employed only in a minority of jurisdictions. It holds that to be liable for negligence, an accountant must be in privity of contract with the plaintiff, or in a third party relationship close enough to approach privity. It is based on a line of New York cases authored by Justice Cardozo, beginning with *Ultramares Corp. v. Touche*,[107] in which the court held that an accountant would only be held liable for negligent misrepresentation to those with whom it was in privity, since to hold otherwise, wrote "may expose accountants to a liability in an indeterminate amount for an indeterminate time to an indeterminate class."[108] Some states apply this standard via statute.[109] Cardozo's opinion distinguished his prior opinion in case of *Glanzer v. Shepard*,[110] in which a buyer of coffee beans brought an action for negligent misrepresentation against a public weigher used by the seller who had certified the wrong weight, resulting in losses to the plaintiff. The weigher was held liable for the

---

[106] DAN L. GOLDWASSER & THOMAS ARNOLD, ACCOUNTANTS' LIABILITY § 4.2[A], at 4-5.

[107] *Ultramares Corp. v. Touche,* 174 N.E. 441 (N.Y. 1931).

[108] *Ultramares Corp. v. Touche,* 174 N.E. 441, 444 (N.Y. 1931).

[109] Six states have statutes limiting the negligence liability of accountants: Arkanas, ARK. CODE. ANN. § 16-114-302 (Michie 1995 Supp.); Illinois, 225 ILL. COMP. STAT. ANN. 450/30.1 (West 1997); Kansas, KAN. STAT. ANN. § 1-402 (1991); New Jersey, NJ STAT. ANN. § 2A:53A-25 (West 1995); Utah, UTAH CODE ANN. § 58-26-12 (1996); and Wyoming, WYO. STAT. ANN. § 33-3-201 (Michie 1995 Supp.). Each of these states limits actions against accountants for negligence, although they have exceptions incorporated into the statute. Arkansas, Illinois, and Utah provide an exception for fraud or intentional misrepresentation, or if the accountant is aware that a primary intent of the client is to use the information for the benefit of the person bringing the suit. Kansas requires that any intended beneficiaries be indentified in writing. New Jersey requires the accountant's knowledge of a specified beneficiary in a specified transaction. Wyoming also requires a specified beneficiary in a specified transaction, but allows the accountant to disclaim any potential liability by placing an appropriate statement to that effect on the document created.

[110] *Glanzer v. Shepard*, 135 N.E. 275 (N.Y. 1922).

misrepresentation even though there was no contract between the weigher and the buyer because the buyer was the direct and intended beneficiary of the information, which created a relationship close enough to privity to impose a duty of care to the buyer.[111] Cardozo held in *Ultramares* that although the relationship between the accountant and those relying on his audit report was "so close as to approach that of privity," the report was prepared for the benefit of the company in privity with the accountant, not any third parties, while in *Glanzer*, the weight certificate was intended for the buyer, and was only incidental to the weigher's contract with the seller.[112]

The two standards remained separate, with *Ultramares* controlling the negligent misrepresentation liability of accountants and other professionals until the Court of Appeals, in *Credit Alliance v. Arthur Andersen & Co.*, combined the two approaches.[113] The court held that accountants would be liable for negligence to third parties not in privity with the accountants who justifiably rely on erroneous information if (1) the accountants were aware of the particular purpose for which the financial reports would be used, (2) the relying parties were known to the accountants, and (3) there was some conduct by the accountants linking them to the relying party and demonstrating their reliance.[114] In addition to New York and the states that have passed statutes limiting accountant liability on this basis,[115] other states have adopted this basic formula, including: California (which had previously been a strict privity state),[116] Connecticut,[117] Idaho,[118] Montana,[119] Nebraska,[120] Pennsylvania,[121] and Virginia.[122]

---

[111] *Glanzer v. Shepard*, 135 N.E. 275, 276 (N.Y. 1922); *see also Credit Alliance v. Arthur Andersen & Co.*, 483 N.E.2d 110, 116-17 (N.Y. 1985).

[112] *Ultramares Corp. v. Touche*, 174 N.E. 441, 446 (N.Y. 1931).

[113] *Credit Alliance v. Arthur Andersen & Co.*, 483 N.E.2d 110, 118 (N.Y. 1985).

[114] *Credit Alliance v. Arthur Andersen & Co.*, 483 N.E.2d 110, 118-19 (N.Y. 1985).

[115] Six states have statutes limiting the negligence liability of accountants: Arkanas, ARK. CODE. ANN. § 16-114-302 (Michie 1995 Supp.); Illinois, 225 ILL. COMP. STAT. ANN. 450/30.1 (West 1997); Kansas, KAN. STAT. ANN. § 1-402 (1991); New Jersey, NJ STAT. ANN. § 2A:53A-25 (West 1995); Utah, UTAH CODE ANN. § 58-26-12 (1996); and Wyoming, WYO. STAT. ANN. § 33-3-201 (Michie 1995 Supp.).

[116] *Bily v. Arthur Young & Co.*, 834 P.2d 745, 752 (Cal. 1992).

[117] *Pasternak v. Colonial Equities Corp.*, 854 F. Supp. 64 (D.C. Conn. 1994) (applying Connecticut law), *claim dismissed sub nom. Seeman v. Arthur Andersen & Co.*, 896 F. Supp. 250 (D.C. Conn.), *affd sub nom. Hirsch v. Arthur Andersen & Co.*, 72 F.3d 1085 (2d Cir. 1995).

[118] *Idaho Bank & Trust Co. v. First Bancorp of Idaho*, 772 P.2d 720 (Idaho 1989).

[119] *Thayer v. Hicks*, 793 P.2d 784 (Mont. 1990).

[120] *Citizens Nat'l Bank of Wisner v. Kennedy and Coe*, 441 N.W.2d 180 (Neb. 1989).

[121] *Landell v. Lybrand*, 107 A. 783 (Pa. 1919).

[122] *Ward v. Ernst & Young*, 435 S.E.2d 628 (Va. 1993).

(2) Reasonable Foreeseeability

A very small number of states, Mississippi[123] and Wisconsin[124] specifically, hold the view that accountants should be liable to all the reasonably foreseeable third parties that rely on their audit reports if the reports were negligently erroneous. This view was first propounded by a judge in a law review article and is based on the rationales that the law has moved away from privity requirements, that accountants are best able to insure against such losses and spread costs around, that the rule best deters negligent conduct by accountants, and that a number of different people rely on audit reports for different reasons.[125] New Jersey also followed this rule until it was superseded by a near privity-style statute in 1995.[126]

(3) Persons Intended or Known --Restatement Approach

By far the majority of state courts[127] have approached accountant negligence by adopting the theory embodied in the Restatement (Second) of Torts, § 552. Unlike the privity or near privity standards, the accountant need not actually know the person relying on the information under the Restatement standard, and is therefore broader. It creates a limited, foreseeable group of people connected to the transaction. However, it is also narrower than the reasonably foreseeable standard, under which it would be impossible to predict how many people might eventually rely on the information. The Restatement approach limits both the group of people connected to the transaction and limits the transactions for which the information might be used. Arguments for the Restatement standard are that it is a moderate view which limits liability a group of persons and transactions the accountant can reasonably predict, that it is less harsh to third party plaintiffs than the privity standards, but is less burdensome to accountants than the

---

[123] *Touche Ross & Co. v. Commercial Union Ins. Co.*, 514 So.2d 315, 321 (Miss. 1987).

[124] *Citizens State Bank v. Timm, Schmidt & Co.*, 335 N.W.2d 361, 366 (Wis. 1983).

[125] *See* Howard B. Wiener, "Common Law Liability of the Certified Public Accountant for Negligent Misrepresentation," 20 San Diego L. Rev. 233 (1983).

[126] *See Rosenblum, Inc. v. Adler*, 93 N.J. 324, 461 A.2d 138 (1983), *superseded by statute, see* N.J. STAT. ANN. § 2A:53A-25 (limiting accountant liability to third parties for negligent acts).

[127] The states which have applied RESTATEMENT (SECOND) OF TORTS § 552 to accountant liability are as follows: Alabama, *Boykin v. Arthur Andersen & Co.*, 639 So.2d 504 (Ala. 1994) (overruling by implication *Colonial Bank v. Ridley & Schweigert*, 551 So.2d 390 (Ala. 1989), which adopted a near privity approach); Alaska, *Selden v. Burnett*, 754 P.2d 256 (Ala. 1988); Georgia, *Badische Corp. v. Caylor*, 356 S.E.2d 198 (Ga. 1987); Hawaii, *Chun v. Park*, 462 P.2d 905 (Hawai'i 1969); Iowa, *Pahre v. Auditor of the State of Iowa*, 422 N.W.2d 178 (Iowa 1988); Kentucky, *Ingram Industries, Inc. v. Nowicki*, 527 F.Supp. 683 (E.D.Ky. 1981); Michigan, *Law Offices of Lawrence J. Stockler, P.C. v. Rose*, 436 N.W.2d 70 (Mich. Ct. App. 1989); Minnesota, *Bonhiver v. Graff*, 248 N.W.2d 291 (Minn. 1976); Missouri, *Mark Twain Plaza Bank v. Lowell H. Listrom & Co.*, 714 S.W.2d 859 (Mo. App. Ct. 1986); New Hampshire, *Spherex, Inc. v. Alexander Grant & Co.*, 451 A.2d 1308 (N.H. 1982); North Carolina, *Raritan River Steel Co. v. Cherry, Bekaert & Holland*, 367 S.E.2d 609 (N.C. 1988); Ohio, *Haddon View Investment Co. v. Coopers & Lybrand*, 436 N.E.2d 212 (Ohio 1982); Pennsylvania, *Coleco Industries, Inc. v. Berman*, 423 F.Supp. 275 (E.D. Pa. 1976), *affirmed in part, remanded in part*, 567 F.2d 569 (3d Cir. 1977), *cert. denied*, 439 U.S. 830 (1978); Rhode Island, *Rusch Factors, Inc. v. Levin*, 284 F.Supp. 85 (D.R.I. 1968); South Carolina, *ML-Lee Acquisition Fund, L.P. v. Deloitte & Touche*, 489 S.E.2d 470, 471 n.3 (S.C. 1997); Texas, *Shatterproof Glass Corp. v. James*, 466 S.W.2d 873 (Tex.Civ.App. 1971); Utah, *Christenson v. Commonwealth Land Title Insurance Co.*, 666 P.2d 302 (Utah 1983); Virginia, *Semida v. Rice*, 863 F.2d 1156 (4th Cir. 1988); and Washington, *TransAmerica Title Insurance Co. v. Johnson*, 693 P.2d 697 (Wash. 1985).

reasonably foreseeable standard. It creates a duty of care "only in circumstances in which the maker was manifestly aware of the use to which the information was to be put and intended to supply it for that purpose." But it is more difficult to apply than the privity standard, and only somewhat less ambiguous than the reasonably foreseeable standard, and it has not been applied consistently among all states, or even all professions.[128]

One commentator posits that "the Restatement rule is difficult to apply to a CA [because the] potential class of persons who will be shown a certificate and asked to rely on it . . . is as large or larger than those who might rely on a report regarding a publicly traded security."[129] The Restatement rule is designed to limit the class of potential litigants to those an accountant can reasonably expect to have relied upon his work. In the context of a certificate, however, limiting the number of persons who may rely on a single certificate would defeat the purpose of having a certificate:

> If Bob acquires a certificate from Alice, that certificate has almost no value to Bob except as a means of facilitating transactions with other parties. Every recipient of a certificate who suffers because of the CA's negligence thus falls squarely within the Restatement (Second) section 552 class of persons who suffer loss "through reliance upon [the negligent misrepresentation] in a transaction that [the CA] intends the information to influence or knows that the recipient so intends or in a substantially similar transaction."[130]

It is unclear how a court would apply this theory with respect to CAs without allowing the entire chain of persons relying on certificates to make a claim for reliance damages should the certificate be erroneous. It is unlikely that courts would want to take any action which would harm a developing industry, but it also means that particular care will need to be taken at the beginning to avoid negligent acts which could lead to liability.

(b) Attorney Liability

Like accountants, attorneys are frequently in positions of trust and confidence, and provide opinions upon which third parties may rely. In his discussion of accountant liability for negligent misrepresentation in *Ultramares Corp. v. Touche*, Justice Cardozo equated the roles of attorneys and accountants in deciding not to extend the scope of negligence liability to third parties not in privity of contract: "Lawyers who certify their opinion as to the validity of municipal or corporate bonds, with knowledge that the opinion will be brought to the notice of the public, will become liable to the investors if they have overlooked a statute or a decision to

---

[128] *See* Gary Lawson & Tamara Mattison, "A Tale of Two Professions: The Third-Party Liability of Accountants and Attorneys for Negligent Misrepresentation," 52 Ohio St. L. J. 1309, 1322-1325 (Winter, 1991); *see also Fireman's Fund Ins. v. SEC Donohue, Inc.*, 679 N.E.2d 1197, 1202 (Ill. 1997) (Heiple, J., dissenting) ("The majority . . . has seen fit to continue a piecemeal approach [to the economic loss doctrine] by applying the *Moorman* doctrine to professional malpractice of architects and now engineers but not attorneys or accountants.")

[129] A. Michael Froomkin, "The Essential Role of Trusted Third Parties in Electronic Commerce," 75 Or. L. Rev. 49, 99 (Spring, 1996).

[130] A. Michael Froomkin, "The Essential Role of Trusted Third Parties in Electronic Commerce," 75 Or. L. Rev. 49, 100-101 (Spring, 1996).

the same extent as if the controversy were one between client and adviser."[131] However, in some recent cases, courts have been extending attorney liability to third parties who rely on information provided by the attorneys, usually in the context of opinion letters.[132]

Although there does not appear to be a clear majority approach, commentators have identified approaches courts have taken in addressing attorney liability to third parties, including the Privity approach, the Restatement approach, the Balancing approach, and the Intended Beneficiary approach, which are similar to the approaches used for accountant liability.[133] They do not use them in exactly the same way, however: "The most dramatic example is Wisconsin, which follows the privity rule for attorneys and the broad foreseeabiliy standard for accountants."[134] Commentators Lawson and Mattison identify the privity rule attorneys are only liable for negligent acts to those with whom they have a contractual relationship or one approaching it, as the most widespread, followed in at least nine states.[135]

The Restatement approach is the most widespread approach addressing accountant liability, but is used less frequently with respect to attorneys. Commentators Lawson and Mattison in 1991 identified only three courts that have used the Restatement approach, one of

---

[131] *Ultramares Corp. v. Touche*, 174 N.E. 441, 448 (N.Y. 1931).

[132] Among the states that have held attorneys liable under a claim of negligent misrepresentation are Georgia, *Williams v. Fortson, Bentley & Griffin*, 441 S.E.2d 686, 688 (Ga. App. Ct. 1994); *Horizon Fin., F.A. v. Hansen*, 791 F. Supp. 1561, 1573-74 (N.D. Ga. 1992) (attorney's opinion letters support negligent misrepresentation claim under Georgia and Pennsylvania law); Illinois, *Geaslen v. Berkson, Gorov & Levin, Ltd.*, 581 N.E.2d 138, 142-43 (Ill. Ct. App. 1991), *aff'd in part, rev'd in part*, 613 N.E.2d 702 (Ill. 1993); Michigan, *Molecular Technology Corp. v. Valentine*, 925 F.2d 910, 915-16 (6th Cir. 1991) (applying Michigan law); New York, *Prudential Ins. Co. of Am. v. Dewey, Ballantine, Bushby, Palmer & Wood*, 605 N.E.2d 318, 320 (N.Y. 1992); New Jersey, *Petrillo v. Bachenberg*, 655 A.2d 1354, 1359 (N.J. 1995); and Oklahoma, *Bradford Secs. Processing Servs., Inc. v. Plaza Bank & Trust*, 653 P.2d 188, 190-91 (Okla. 1982).

[133] *See* Gary Lawson & Tamara Mattison, "A Tale of Two Professions: The Third-Party Liability of Accountants and Attorneys for Negligent Misrepresentation," 52 Ohio St. L. J. 1309, 1322 (Winter, 1991); *see also* Robert L. Paddock, Note, "Liability of Attorneys to Third Parties Through Opinion Letters: A Well-Intentioned Rule Which May Stifle the Legal Profession if Not Modified," 38 S. Tex. L. Rev. 325 (March, 1997); Jonathan J. De Jong, "Attorney Liability to Third Party Non-Clients," 5 Kan. J.L. & Pub. Pol'y 161, 162 (Fall, 1995).

[134] Gary Lawson & Tamara Mattison, "A Tale of Two Professions: The Third-Party Liability of Accountants and Attorneys for Negligent Misrepresentation," 52 Ohio St. L. J. 1309, 1323 & nn.62-63 (Winter, 1991) (citations omitted).

[135] *See* Gary Lawson & Tamara Mattison, "A Tale of Two Professions: The Third-Party Liability of Accountants and Attorneys for Negligent Misrepresentation," 52 Ohio St. L. J. 1309, 1323 & nn.61 (Winter, 1991). Among these states are: Florida, *Moss v. Zafiris*, 524 So. 2d 1010, 1011 (Fla. 1988); Illinois, *McLane v. Russell*, 546 N.E.2d 499, 501-02 (Ill. 1989); Indiana, *Ackerman v. Schwartz*, 733 F. Supp. 1231, 1241-43 (N.D. Ind. 1989) (applying Indiana law), *appeal dismissed*, 922 F.2d 843 (7th Cir. 1991); Louisiana, *Abell v. Potomac Ins. Co.*, 858 F.2d 1104, 1131-33 (5th Cir. 1988) (applying Louisiana law), *cert. denied*, 492 U.S. 918 (1989); Maryland, *Flaherty v. Weinberg*, 492 A.2d 618, 625-26 (Md. 1985); Massachusetts, *Robertson v. Gaston Snow & Ely Bartlett*, 536 N.E.2d 344, 348 (Mass. 1989), *cert. denied*, 493 U.S. 894 (1989); Minnesota, *Schuler v. Meschke*, 435 N.W.2d 156, 162-63 (Minn. Ct. App. 1989); *Citizens Nat'l Bank v. Kennedy & Coe*, 441 N.W.2d 180, 182 (Neb. 1989); New York, *Council Commerce Corp. v. Schwartz, Sachs & Kamhi, P.C.,* 534 N.Y.S.2d 1, 2 (N.Y.A.D. 2 Dept. 1988), *appeal denied*, 534 N.E.2d 85 (N.Y. 1989); Texas, *First Mun. Leasing v. Blankenship, Potts, Aikman, Hagin & Stewart*, 648 S.W.2d 410, 413 (Tex. Ct. App. 1983); and Wisconsin, *Green Spring Farms v. Kersten*, 401 N.W.2d 816, 822-27 (Wis. 1987).

which appeared to be more of a privity rule in that the court found that the attorney had no duty to third party plaintiffs.[136] Colorado recently adopted a Restatement approach for determining the liability of attorneys to third parties, and overturned a summary judgment ruling on the ground that the courts should have applied Section 552 in ruling on the plaintiff's negligent misrepresentation claim.[137]

The Balancing approach is based on the factors identified by the California Supreme Court in *Biakanja v. Irving*,[138] a negligent misrepresentation case involving a notary engaged in the unauthorized practice of law in drafting a will, which was extended to attorneys in the case *Lucas v. Hamm*.[139] The factors identified as necessary to weigh before imposing liability on an attorney based on a third party claim include: "the extent to which the transaction was intended to affect the plaintiff, the foreseeability of harm to him, the degree of certainty that the plaintiff suffered injury, the closeness of the connection between the defendant's conduct and the injury suffered, the moral blame attached to the defendant's conduct, and the policy of preventing future harm."[140] It is a difficult test to apply, and although it is used in California,[141] it has been criticized by other courts.[142]

The Intended Beneficiary test arose out of the wills and trusts context for negligent drafting of instruments, in which it was a relatively straightforward matter to identify the intended beneficiary.[143] Expanding the rule beyond that context, however, is difficult in the context of attorneys and opinion letters. It therefore remains unclear which direction most courts will take in holding attorneys liable to third parties for negligent misrepresentation.

(c) Notary Public Liability

A notary must perform his duties with "honesty, integrity, diligence, and skill."[144] Currently, notaries are held liable, either by statute,[145] or case law,[146] for any damages caused by

---

[136] See Gary Lawson & Tamara Mattison, "A Tale of Two Professions: The Third-Party Liability of Accountants and Attorneys for Negligent Misrepresentation," 52 Ohio St. L. J. 1309, 1323-24 (Winter, 1991); *Eisenberg v. Gagnon*, 766 F.2d 770, 779-80 (3d Cir.), *cert. denied sub nom. Waserstrom v. Eisenberg*, 474 U.S. 946 (1985); *Garcia v. Rodey, Dickason, Sloan, Akin & Robb*, 750 P.2d 118 (N.M. 1988); *see also Collins v. Binkley*, 750 S.W.2d 737, 738-39 (Tenn. 1988).

[137] *Mehaffey, Rider, Windholz & Wilson v. Central Bank Denver, N.A.*, 892 P.2d 230, 236 (Colo. 1995).

[138] *Biakanja v. Irving*, 320 P.2d 16, 18 (Cal. 1958).

[139] *Lucas v. Hamm*, 364 P.2d 685, 687 (Cal. 1961) (en banc).

[140] *Biakanja v. Irving*, 320 P.2d 16, 19 (Cal. 1958).

[141] *See, e.g., Roberts v. Ball, Hunt, Hart, Brown & Baerwitz*, 57 Cal. App. 3d 104, 110-11 (Cal. Ct. App. 2 Dist. 1976).

[142] *See, e.g., Pelham v. Griesheimer*, 440 N.E.2d 96, 100 (Ill. 1982); *Donohue v. Shughart, Thompson & Kilroy, P.C.*, 900 S.W.2d 624, 629 (Mo. 1995) (refusing to apply the balancing test to attorneys, although it is applied to accountants).

[143] *See, e.g., Wisdom v. Neal*, 568 F. Supp. 4, 8 (D. N.M. 1982); *Auric v. Continental Cas. Co.*, 331 N.W.2d 325, 329 (Wis. 1983).

[144] *Hungate v. Indemnity Ins. Co. of N. Amer.*, 18 P.2d 64, 64 (Cal. App. Ct., 4 Dist. 1933).

their official misconduct.[147] Notaries owe a duty of care to any persons, including third parties, who rely on official notarial statements,[148] based on their status as public officials, to refrain from negligent, reckless, or willfully injurious conduct in the performance of their notarial functions.[149] A notary may therefore be liable under tort for negligent, willful or reckless breaches of this duty of care to those who actually rely on the fact of the notarization of a signature.

(d) Financial Information Providers

Financial information about companies, stock and bond prices, and other indexes of financial information is compiled by specialist companies which then provide such information to subscribers. Whether a company has a special relationship with a particular person or is a general publisher of information is a significant factor in determining whether such companies may be held liable for erroneous information which is then relied on by investors in making decisions about entering certain business transactions. Some disseminators of financial information have been held liable for negligent misrepresentation when they have been sufficiently aware of particular parties who might foreseeably rely on such information to their

---

[145] The Model Notary Act has a section which states "A notary is liable to any person for all damages proximately caused that person by the notary's official misconduct in performing a notarization." Model Notary Act, § 6-101(a). Other states have similar provisions. See, e.g., Illinois Notary Public Act, "Cause of Damages," 5 ILL. COMP. STAT. ANN. 312/7-103 (West 1997) ("It is not essential to a recovery of damages that a notary's official misconduct be the only cause of the damages.").

[146] *See, e.g., Independence Leasing Corp. v. Aquino*, 506 N.Y.S.2d 1003 (N.Y. Co. Ct. 1986) (negligence has long been within the scope of notary misconduct, and no exemption is allowed due to official nature of notarial acts).

[147] "Official misconduct" includes "wrongful" acts in the performance of a duty, and includes acts which are "unauthorized, unlawful, abusive, negligent, reckless, or injurious." 5 ILL. COMP. STAT. ANN. 312/7-104 (West 1997).

[148] *Immerman v. Ostertag*, 199 A.2d 869, 872-73 (N.J. 1964); *see also Independence Leasing Corp. v. Aquino*, 506 N.Y.S.2d 1003 (N.Y. Co. Ct. 1986); CAL. GOV. CODE § 8214 (West 1997) ("For the official misconduct or neglect of a notary public . . . [the notary is] liable in a civil action to the persons injured thereby for all the damages sustained."); *Biakanja v. Irving*, 320 P.2d 16 (Cal. 1958) (notary liable to third party for losses due to unauthorized practice of law in drafting a will); 66 C.J.S. "Notaries" § 10 ( ) ("[A notary's] duty is not confined to the one to whom he directly renders service, but it extends to all persons who may be affected by his act.")..

[149] *E.g.*, ALASKA STAT. § 44.50.160; CAL. GOV'T CODE § 8214; COLO. REV. STAT. § 12-55-116; CONN. GEN. STAT. ANN. § 3-941; FLA. STAT ANN. §§ 117.05, -.105; HAW. REV. STAT. ANN. § 456-6; IDAHO CODE § 51-118; N.Y. EXEC. LAW. § 6-135; UTAH CODE ANN. § 46-1-15; VT. STAT. ANN. tit. 24, § 446. For case law, *see Beneficial Mortgage Co. v. Powers*, 550 N.E.2d 793 (Ind. Ct. App. 1990) (no cause of action for loss when mortgage company did not rely on negligent notarization; injury not proximately caused by negligent act); *Kirk Corp. v. First Am. Title Co.*, 270 Cal. Rptr, 24 (Cal. Ct. App. 1 Dist. 1990) (liability of notary predicated on proximately caused injury by negligent act); *Garton v. Title Ins. and Trust Co.*, 165 Cal. Rptr. 449 (Cal. Ct. App. 3 Dist. 1980) (negligent notary liable for all proximately caused injuries); *Tutelman v. Agricultural Ins. Co.*, 102 Cal. Rptr. 296 (Cal. Ct. App. 2 Dist. 1972) (notary's negligence need not be sole proximate cause of loss; need only show notary's negligence joined to proximately cause injury). *See also Marine Midland Bank v. Stanton*, 556 N.Y.S.2d 815 (N.Y. Sup. 1990) (notarial misconduct includes negligent, willful or fraudulent acts); *Summers Bros., Inc. v. Brewer*, 420 So. 2d 197 (La. Ct. App. 1 Cir. 1982) (notary liable for all damages proximately caused by misfeasance).

detriment to create a special relationship,[150] but have been held not liable when they were in the position of a general publisher, and could not know who might rely on erroneous information.[151]

Courts are generally unwilling to hold newspapers or similar entities liable for errors under a negligent misrepresentation theory, even if someone relies on the information, because policy considerations argue against holding information suppliers liable to such an indeterminate and inexhaustible class of plaintiffs, which could easily put such companies out of business.[152] Further, the fact that the information is directed to the general public rather than the particular needs of a single person or smaller group of people means that a publisher has no duty to its general audience which would support a claim of liability for a breach by a negligent misrepresentation.[153] Financial information is treated as generally published information despite the fact that investors may rely on it in making business decisions. In *Jaillet v. Cashman*, a New York court held that Dow, Jones & Co. was not liable for incorrect information reported on a ticker tape, which caused the plaintiff to sell certain stocks, resulting in an economic loss. The court held that a provider of financial information was in the same relationship to the public as a newspaper, and there could be no liability for negligence absent a contractual or other special relationship.[154]

However, where a CA knows that a particular limited group of persons may rely on certain information, liability for negligent misrepresentation becomes likelier. This may be especially true for erroneous listing or failure to list a certificate on CRLs. Here, the CA may be found liable for any negligence to those harmed by relying on the information.

In another case, the court granted a new trial to a plaintiff who alleged reliance on certificates issued by the defendant attached to bonds. The certificates referred to a separate Collateral Trust Indenture which said that the bonds were secured by notes and guaranteed by the defendant. The collateral turned out to be worthless.[155] The court held the defendant liable based on negligent misrepresentation because, under the rule of *Glanzer v. Shepard*, the relationship between the parties was close enough to contractual privity to create a duty of care in the defendant to act reasonably in making statements: "the defendant knew that the certificates were desired for a serious purpose by persons who intended to rely and act thereupon. They were issued for the very purpose of establishing a relationship . . . between the defendant and the persons who might rely thereon."[156] The court found the misrepresentations to be the

---

[150] *Doyle v. Chatham & Phenix Nat. Bank*, 171 N.E. 574 (N.Y. 1930).

[151] *Gutter v. Dow Jones, Inc.*, 490 N.E.2d 898 (Ohio 1986).

[152] *Gutter v. Dow Jones, Inc.*, 490 N.E.2d 898, 902 (Ohio 1986).

[153] *Demuth Development Corp. v. Merck & Co., Inc.*, 432 F. Supp. 990, 992-93 (E.D.N.Y. 1977).

[154] *Jaillet v. Cashman*, 115 Misc. 383, 383-84 (N.Y. Sup. Ct. 1921); *see also First Equity Corp. of Florida v. Standard & Poor's Corp.*, 869 F.2d 175, 179 (2d Cir. 1989); *Gutter v. Dow Jones, Inc.*, 490 N.E.2d 898 (Ohio 1986); *Demuth Development Corp. v. Merck & Co., Inc.*, 432 F. Supp. 990, 992-93 (E.D.N.Y. 1977).

[155] *Doyle v. Chatham & Phenix Nat. Bank*, 171 N.E. 574, 575 (N.Y. 1930).

[156] *Doyle v. Chatham & Phenix Nat. Bank*, 171 N.E. 574, 579 (N.Y. 1930).

proximate cause of the plaintiff's loss because if the certificates had not been issued, the bonds would not have issued and the plaintiffs could not have invested in them.[157]

Standard & Poor's (S&P) was held to have a duty to third party members of the Chicago Board Options Exchange (CBOE) for special reports of stock indexes which contained erroneous information, but which were relied on by the plaintiff to calculate option contract values for settlement. Although the indexes were the subject of a licensing agreement between Standard & Poor's and the CBOE, which exculpated S&P for any errors or inaccuracies, their use was also required by the rules of the CBOE.[158] The court held that S&P owed a duty of care as an information supplier to those it knew would reasonably rely on the information, including the plaintiff: "S&P has specifically contracted to provide information upon which, to a certainty, investments will be encouraged and determined solely on the basis of S&P index values. Users of the information are not casual passersby . . ."[159] Similarly, a court found that a claim was sufficiently stated against a bond rating service for failing to exercise reasonable care in obtaining the necessary information to rate a private bond issue, and because the rating it provided may have negligently misrepresented the financial risk of the bonds.[160] The court held that Moody's Investors Service intended for potential purchasers to rely on its ratings.[161]

(e) Credit Reporting Agencies

Credit Reporting agencies are responsible for verifying and reporting information about the financial status of consumers. They may face liability for negligence in collecting and verifying information about the financial or credit status of those whom they report on. Such claims, however, will be based on the Fair Credit Reporting Act ("FCRA"), which provides civil liability for negligence in failing to comply with any provision of the act, rather than common law tort negligence.[162] Additionally, the FCRA only applies to negligent reports used in consumer transactions, not commercial transactions.[163] Therefore, while the basis for liability for negligent credit reporting ,may be analogous and similar to that faced by CAs, the FCRA will not be applied to CAs.

However, CAs perform identity verification functions similar to those performed by credit reporting agencies, and may face liability for failures to correct erroneous information. The FCRA requires that credit reporting agencies maintain "reasonable procedures" to insure that they are in compliance with the act.[164] CAs may have a duty to use reasonable procedures in

---

[157] *Doyle v. Chatham & Phenix Nat. Bank*, 171 N.E. 574, 575 (N.Y. 1930).

[158] *Rosenstein v. Standard & Poor's Corp.*, 636 N.E. 2d 665, 666-68 (Ill. App. Ct. 1 Dist 1993).

[159] *Rosenstein v. Standard & Poor's Corp.*, 636 N.E. 2d 665, 669-70 (Ill. App. Ct. 1 Dist 1993).

[160] *Fidelity State Bank & Trust Co. v. Merrill Lynch, Pierce, Fenner, & Smith, Inc.*, 768 F. Supp. 300 (D. Kan. 1991).

[161] *Fidelity State Bank & Trust Co. v. Merrill Lynch, Pierce, Fenner, & Smith, Inc.*, 768 F. Supp. 300 (D. Kan. 1991).

[162] 15 U.S.C. § 1681o (West 1997) ("Civil liability for negligent noncompliance").

[163] *Podell v. Citicorp Diners Club, Inc.*, 914 F. Supp. 1025, 1036-37 (S.D.N.Y. 1996).

[164] *See Pettus v. TRW Consumer Credit Service*, 879 F. Supp. 695, 697 (W.D. Tex 1994).

their collections and dissemination of certificate information as well. Errors in a report do not create strict liability, but a consumer may have a remedy for any actual damages suffered as a result of the reporting agency's negligence.[165] To prove negligence under the FCRA, a plaintiff must show that he suffered actual damages proximately caused by the agency's negligence in reporting or investigating erroneous information.[166]

Credit reporting agencies have faced significant liability for damages caused by negligence in investigating and correcting erroneous information. In *Stevenson v. TRW, Inc*., the reporting agency was negligent in investigating and correcting unverifiable and incorrect information regarding the plaintiff, based on the agency's confusion of the plaintiff with his son, who shared his name. Because of the failure of TRW to both properly verify the person to whom the bad accounts actually belonged, or to investigate fraudulent activity by the son, the Fifth Circuit awarded the plaintiff $30,000 for mental anguish suffered and $20,700 in attorney's fees. The court found that the agency was negligent in failing to follow reasonable verification procedures: the agency did not call creditors for information about the accounts, they took an "unreasonably long" time (several months) to reinvestigate disputed information, they failed to delete the information from his report, which reappeared in several reports, and they failed to provide sufficient notice of rights on their standard form, as required by the FCRA.[167] The mental anguish was due to the shock the plaintiff, a 78-year-old man, suffered upon receiving a bad report, significant time expended on trying to clear up the mistakes, three denials of credit after maintaining a clear report for some 60 years, and embarrassment in having to explain to several business associates and creditors why he had a bad report.[168]

Similarly, a court denied a motion to dismiss based on such facts as that a credit reporting agency reported that the plaintiff was a convicted felon without checking other identifying features or corroborating circumstances other than that they shared the same name, even though their birth dates differed, and even after conducting a "reinvestigation."[169] The court found these to be sufficient allegations to state a cause of action against the credit reporting agency for both negligent and willful noncompliance with the FCRA.[170]

4.3.3 Duty to Victims

An interesting question is raised as to whether so-called "third party victims" have a claim for negligent misrepresentation. Third party victims are persons whose identity is included on a certificate obtained by an imposter. The imposter is then able to use the certificate to pose as the third party victim in entering into a presumably fraudulent transaction. In such a case, there is no question that the certificate constitutes a misrepresentation of identity. Assuming for the sake of argument that the certificate was issued as a result of the certification authority's

---

[165] *Pettus v. TRW Consumer Credit Service*, 879 F. Supp. 695, 697 (W.D. Tex 1994).

[166] *Pettus v. TRW Consumer Credit Service*, 879 F. Supp. 695, 698 (W.D. Tex 1994).

[167] *Stevenson v. TRW, Inc.*, 987 F.2d 288, 293, 296-98 (5th Cir. 1993).

[168] *Stevenson v. TRW, Inc.*, 987 F.2d 288, 293, 298 (5th Cir. 1993).

[169] *Stevenson v. Employers Mut. Ass'n*, 960 F. Supp. 141, 143-44 (N.D. Ill. 1997).

[170] *Stevenson v. Employers Mut. Ass'n*, 960 F. Supp. 141, 143-44 (N.D. Ill. 1997).

negligent failure to exercise due care, and that the victim (whose identity was misappropriated) was injured, there is still an argument that the third party victim did not "rely" on the misrepresentation, and therefore, has no claim for misrepresentation.[171]

At least one case supports this conclusion. In *King v. Crossland Savings Bank*,[172] the court found that plantiff's recovery on a negligent misrepresentation claim was precluded by the fact that they did not rely on the representation made by the defendant. In that case, American Express furnished information to a bank, at the bank's request, concerning travellers checks that the plainttfs were presenting for payment. The information incorrectly indicated that the checks were stolen, and this error led to the arrest of the plantiffs. The court rejected plaintiffs' negligent misrepresentation claim under New York law, because, in effect, American Express owed no duty of care to the parties cashing the checks. The court noted that the plaintiffs must prove "reliance" and that here, the injured parties did not rely. As the court noted, under New York law, "a cause of action for negligent misrepresentation can be maintained only when the plaintiff *himself or herself* relies on statements made by the *defendant*[173]. Here, the court noted, the plaintiffs did not rely on the representations made by the defendant.

A contrary view, however, was expressed in the case of *Testa v. Wynquist*.[174] In that case, the plaintiff alleged numerous harms flowing from his false arrest by police who had relied on information erroneously provided by the National Computer Information Center (NCIC) -- a non-state private entity which kept computerized records on cars reported as stolen. The *Testa* court allowed a third party action by the police against the NCIC to proceed because the court found that the plaintiff could have brought an action against the NCIC for failure to store accurate information. ("when breach of this duty to maintain accurate records results in a false or unconstitutional arrest . . ., the arrestee has a cause of action against those who breached this duty.")

In acknowledging a duty to maintain accurate records, the *Testa* court addressed the issued of whether a defendant who arguably has a duty to provide accurate information may nonetheless escape liability because the plaintiff did not directly rely on the defendant's misrepresentation. The *Testa* court found that such a defendant could not escape liability.

4.4 Endorser Liability

In addition to liability for negligent misrepresentation based upon statements made in certificates issued by the CA, there exists the possibility that the use of CA branded certificates by subscribers (such as to validate the identity of their Web site or to validate the identity of their

---

[171] RESTATEMENT (SECOND) OF TORTS § 552(1) (1977) covers loss suffered by the plaintiff as a result of its "justifiable reliance on the information."

[172] *King v. Crossland Savings Bank*, 111 F.3d 251 (2d Cir. 1997),

[173] See also, *Williams v. State*, 98.D.2d 861, 456 N.Y.S.2d 491, 493 (Third Department, 1982) (holding that a claim for negligent misrepresentation could not stand where the police, not the plaintiff, relied on statements made by the DMV).

[174] *Testa v. Wynquist*, 451 F. Supp. 388 (D. R.I. 1978).

own certification authority business) may be construed as an endorsement of the subscriber by the CA in a manner that would constitute negligent misrepresentation.

A line of cases holds that endorsers of products may be liable for negligent misrepresentation if the product fails to live up to the justifiable expectations of quality created by the endorsement and a consumer is harmed by relying on that endorsement. Independent testing laboratories such as Underwriters Laboratory,[175] magazines which endorse products such as Good Housekeeping,[176] and trade associations which lend their mark to products[177] have all been held liable for negligent misrepresentation when the products failed to meet expectations. A certificate itself may be considered an endorsement by the CA of the digital signature or Web site that it is used to verify. That is, the CA may be perceived as lending its reputation and mark to the transaction for the purpose of building trust -- conduct that makes the CA analogous to an endorser.

The majority of courts have held that endorsers are not liable for strict products liability or breach of warranty if they did not participate in the manufacture or distribution of the product.[178] Generally, they are held liable for negligence only if a duty is found to the ultimate consumer.[179] This duty may arise by undertaking an endorsement in the first place, especially if testing is involved. In one case, Underwriters Laboratory was held liable in negligence for allowing a negligently designed fire extinguisher to bear its mark because the label stated that it had been inspected and tested under certain conditions by UL, but the product was later found to have a design defect which caused it to fail under certain conditions.[180] UL was held liable for negligence in approving the design and endorsing the product. Although UL did not have a duty to act in the first place, once it undertook to inspect the product, it undertook a duty of reasonable care to any parties later harmed by the product.[181] In a later case, Underwriters Laboratory was

---

[175] *Hempstead v. General Fire Extinguisher Corp.*, 269 F. Supp 109 (D.C. Del. 1967).

[176] *Hanberry v. Hearst Corp.*, 276 Cal. App. 2d 680 (Cal. App. Ct. Dist. 4 1969).

[177] *King v. Nat'l Spa and Pool Inst., Inc.*, 570 So.2d 612 (Ala. 1990).

[178] Holly Peihler Rockwell, "Products Liability of Endorser, Trade Association, Certifier, or Similar Party Who Expresses Approval of Product," 1 ALR5th 431, 439 (1992).

[179] Holly Peihler Rockwell, "Products Liability of Endorser, Trade Association, Certifier, or Similar Party Who Expresses Approval of Product," 1 ALR5th 431, 440 (1992). States finding a duty to a consumer for an endorser's representation include: Alabama, *King v. National Spa & Pool Inst., Inc.*, 570 So.2d 612 (Ala. 1990) (trade association); California, *Hanberry v. Hearst Corp.*, 276 Cal. App. 2d 680 (Cal. App. Ct. Dist. 4 1969) (magazine publisher); Illinois, *Yassin v. Certified Grocers of Illinois, Inc.*, 502 N.E.2d 315 (Ill. App. Ct. 1 Dist 1986) (independent testing laboratory); New Jersey, *Yuhas v. Mudge*, 322 A.2d 824 (N.J. Super. A.D. 1974) (magazine publisher), *Myers v. Donnatacci*, 531 A.2d 398 (N.J. Super. 1987) (trade association); New York, *Beasock v. Dioguardi Enterprises, Inc.*, 130 Misc.2d 25 (N.Y. Super.), *revd on other grounds*, 499 NYS2d 558 (N.Y. Super. 4 Dept. 1986) (trade association), *Howard v. Poseidon Pools, Inc.*, 506 NYS2d 523 (N.Y. Super. 1985), *affd in part and revd in part on other grounds*, 522 NYS2d 388 (N.Y.A.D. 4 Dept. 1986) (trade association), Pennsylvania, *Friedman v. F.E. Myers Co.*, 706 F. Supp. 376 (E.D. Pa. 1989) (applying Pennsylvania law) (trade association); Virginia, *Hempstead v. General Fire Extinguisher Corp.*, 269 F. Supp 109, 117 (D.C. Del. 1967) (applying Virginia law) (independent testing laboratory); and Washington, *Rottinghaus v. Howell*, 666 P.2d 899 (Wash. Ct. App. Div. 3), *review den* 100 Wash.2d 1016 (Wash. 1983) (seed certifier).

[180] *Hempstead v. General Fire Extinguisher Corp.*, 269 F. Supp 109, 117 (D.C. Del. 1967) (applying Virginia law).

[181] *Hempstead v. General Fire Extinguisher Corp.*, 269 F. Supp 109, 118 (D.C. Del. 1967).

found not liable because its published standards were clear, but those standards were not followed by the manufacturer, even though UL had provided an endorsement for the product.[182] An endorser, therefore will only be held liable for its own failings, such as negligence in creating standards which others follow and which result in harm, or a failure to follow its own testing procedures and standards if they undertake testing before providing an endorsement.

Good Housekeeping magazine was held to have a duty of care to those consumers who rely on its "Good Housekeeping Seal of Approval" endorsement in selecting products, even though Good Housekeeping has no direct relationship to the buyer.[183] The California Supreme Court held that a claim for negligent misrepresentation against Good Housekeeping's publisher was appropriate for injuries caused by a potential design defect in a pair of shoes which the plaintiff bought in reliance on the Good Housekeeping Seal of Approval. The court held that the fact that Good Housekeeping had voluntarily put itself in the marketing process, and loaned its reputation to promote the use of a product, meant that it had assumed a duty of ordinary care to consumers with respect to awarding the seal to particular products.[184] "The fact Hearst [the publisher] is not in privity of contract with those who, relying on its endorsement, purchase the products it endorses, does not mean it is relieved of the responsibility to exercise ordinary care toward them."[185]

However, the court was not willing to hold Good Housekeeping ultimately liable for strict product liability or breach of warranty claims, which would make the magazine liable if the individual shoes bought by the plaintiff, rather than the design of the product generally, were defective. The court was not willing to hold the magazine to the same standard of care as the manufacturer who actually produces the shoes. The court held that this would go way beyond the role required of a "general endorser who makes no representation it has examined or tested each item marked," as manufacturers generally do.[186] Rather, the court held that Good Housekeeping could only be held liable to the extent of its representation, if the plaintiff could prove that it was negligent in making that representation.[187] "The most that can be implied from respondent's representation is that it has examined or tested samples of the product and found the general design and materials used to be satisfactory."[188]

The conclusion of this case makes clear that the CA must carefully delineate the nature of the representation it is making with respect to the certificates it issues (and the use of the CA logo on subscriber web sites, if allowed). Such representations should be clearly stated in the

---

[182] *Benco Plastics, Inc. v. Westinghouse Electric Corp.*, 387 F. Supp. 772, 778-79 (E.D. Tenn. 1974).

[183] *Hanberry v. Hearst Corp.*, 276 Cal. App. 2d 680 (Cal. App. Ct. Dist. 4 1969).

[184] *Id.* at 178-79.

[185] *Id.* at 177.

[186] *Id.* at 180.

[187] *See also, McCulloch v. Ford Dealers Advertising Assn' of So. Cal.*, 234 Cal. App. 3d 1385 (Cal. Ct. App. 4 Dist. 1991) (Sponser of auto race not liable for negligent misrepresentation for promotional materials which used its logo; duty to investigate promotional claims may have existed, but causation between injuries and association's involvement was too remote to allow recovery).

[188] *Id.* at 179.

CA's certificate policy or certification practice statement or otherwise clearly publicized. See section 4.6 for discussion as to when, and under what circumstances, such notice is adequate.

A trade association may be held liable as an endorser, especially if the association members promulgate design or manufacture standards for products, and certify particular products as having been manufactured in accordance with those standards. An association will not be held liable for failure to promulgate standards, which is a voluntary act by the association, but if it does provide standards, it may be liable if the standards are found to have been negligently created, or are not updated periodically.[189] In one case, for example, a trade association was found potentially liable for negligence in putting forth standards that, even though followed by the manufacturer of a pool, resulted in the death of the pool's owner from diving from the diving board. The plaintiff argued that the placement of the diving board following the specifications of the standards created an unreasonable risk of harm and that the association was negligent in approving standards that could result in such harm. The court held that the association could be held liable for the standards it put forth, and that because it was lending its reputation to a product for the purposes of making that product more attractive to consumers, it created a legal duty to use reasonable care to prevent consumers from being harmed by their reliance on the supposedly expert advice of that association, especially where one of the purposes for creating the standards was supposedly to increase the safety of the consumer in using pools.[190]

Although the trade association had no legal or statutory obligation to undertake to provide such standards, once they did so, they created a duty to all those who might rely on those standards that the standards were created using reasonable care to prevent risk of harm.[191] The court was unpersuaded by the argument that the association could not oversee the use of the standards by its members: "In our view . . . the fact that a trade association does not specifically control the action of its members does not, as a matter of law, absolve the trade association of a duty to exercise reasonable care when it undertakes to promulgate standards for the 'needs of the consumer.'"[192] Therefore, to the extent that a CA establishes standards for the certification of digital transactions, it may face some liability if those standards, even as used by other entities such as member banks, turn out to create an unreasonable risk of loss due to negligence. However, if such procedures are not negligently created, but are simply misused by others, the CA should not face liability.

4.5 Economic Loss Doctrine

A CA's liability for tort claims based on negligence may be limited by the so-called "economic loss doctrine". The economic loss doctrine provides that claims for purely economic losses for product defects are not recoverable in tort.[193]

---

[189] *King v. Nat. Spa and Pool Inst.*, 570 So.2d 612 (Ala. 1990).

[190] *King v. Nat. Spa and Pool Inst.*, 570 So.2d 612 (Ala. 1990).

[191] *King v. Nat. Spa and Pool Inst.*, 570 So.2d 612 (Ala. 1990).

[192] *King v. Nat. Spa and Pool Inst.*, 570 So.2d 612 (Ala. 1990).

[193] Reeder R. Fox and Patrick J. Loftus, "Riding the Choppy Waters of East River: Economic Loss Doctrine Ten Years Later," 64 Def. Couns. J. 260, 260 (April, 1997).

The idea of an economic loss rules stems primarily from modern case law dealing with product liability torts involving mass market goods. The rule holds simply that tort liability does not arise for pure economic loss, but only for personal injury or property damage. The basic theme encompassed in this rule is that personal injury and property damage claims engage far more important social policies than do pure economic (business) losses. Equally important, parties are often able to allocate risk and loss by contract pertaining to economic variables and, thus, an economic loss exclusion serves to allocate responsibility and the scope of application between contract and tort law. While the economic loss rule is not universally adopted, its influence extends broadly into the majority of all states and is growing.[194] Some states apply the doctrine to services and to negligent misrepresentation claims.[195] However, some states provide exceptions to the economic loss doctrine which may apply as well, and allow tort claims for purely economic losses. There is little consistency as to how it is applied from state to state,[196] and some states allow significant exceptions to the doctrine,[197] while other states do not allow its application at all.[198]

The economic loss doctrine is a judicial policy doctrine developed by the courts to prevent the shading of law into tort and away from contract. It reflects reasoning by the courts that "tort law would, if allowed to develop unchecked, eventually envelop contract law."[199] The economic loss doctrine says that there is no recovery in tort available for purely economic losses, since those are better covered by contract or warranty. Because digital certificates of the type to be issued by the CA will almost exclusively involve financial and commercial transactions, and would only rarely, if ever, be linked with physical injury or damages to other property, the economic loss doctrine may frequently apply to actions brought against certification authorities for tort damages.[200] In one case, for example, the Eighth Circuit held that the failure of a pharmacy's customized computer system was an economic loss, that an action in negligence was barred by the economic loss doctrine and that recovery was limited to contractual remedies.[201] If

---

[194] NIMMER, INFORMATION LAW at ¶10.16 at 10-65.

[195] Reeder R. Fox and Patrick J. Loftus, "Riding the Choppy Waters of East River: Economic Loss Doctrine Ten Years Later," 64 Def. Couns. J. 260, 260 (April, 1997).

[196] *See, e.g.*, Reeder R. Fox and Patrick J. Loftus, "Riding the Choppy Waters of East River: Economic Loss Doctrine Ten Years Later," 64 Def. Couns. J. 260, 270 (April, 1997) ("because of differing interpretations as to the applicability and interpretation of the [economic loss] doctrine, practitioners would be well advised to make a careful check of the law in the applicable jurisdiction before relying on this defense.").

[197] Illinois applies the economic loss doctrine to cases involving both products and services, but with three significant exceptions: (1) where personal injury or property damage was suffered due to a sudden and dangerous occurrence, such as brake failure; (2) where damages are the result of intentional false misrepresentation; or (3) damages caused "where one who is in the business of supplying information for the guidance of others in their business transactions makes negligent representations." *Moorman Mfg. Co. v. National Tank Co.*, 435 N.E.2d 443, 448, 452 (Ill. 1982); *see also Fireman's Fund Ins. v. SEC Donohue, Inc.*, 679 N.E.2d 1197, 1199-1200 (Ill. 1997).

[198] See Christopher Scott D'Angelo, "The Economic Loss Doctrine: Saving Contract Warranty Law From Drowning in a Sea of Torts. 6 U.Tol.L. Rev. 591, 608 Appendix A (Spring, 1995).

[199] *Fireman's Fund Ins. v. SEC Donohue, Inc.*, 679 N.E.2d 1197, 1199 (Ill. 1997) (quoting *Congregation of the Passion, Holy Cross Province v. Touche Ross & Co.*, 636 N.E.2d 503 (Ill. 1994)).

[200] *See Rockport Pharmacy, Inc. v. Digital Simplistics, Inc.*, 53 F.3d 195 (8th Cir. 1995).

[201] *Rockport Pharmacy, Inc. v. Digital Simplistics, Inc.*, 53 F.3d 195, 198 (8th Cir. 1995).

the economic loss doctrine is found to apply to tort actions against CAs, it will prevent recovery on that basis, even in the absence of a contract.[202]

The economic loss doctrine grows out of products liability and is based on the theory that, even if a product is defective, there is no strict liability recovery in tort when there is no physical or property damages to others. It was established by the case of *Seely v. White Motor Co*., in which the California Supreme Court held that a plaintiff could not recover in a tort negligence action for a defective truck which did not injure anyone, but only needed repairs after crashing due to defective brakes.[203] The court held that the losses suffered by the plaintiff were economic only, and due to the failure of the product to live up to the buyer's expectations.[204] The United States Supreme Court accepted this doctrine in a case involving damages to turbines caused by a defective design, and a negligence action brought for the cost of repairs.[205] The Supreme Court explained that "when a product injures itself, the commercial user stands to lose the value of the product, risks the displeasure of its customers who find that the product does not meet their needs, or, as in this case, experiences increased costs in performing a service," and held that the manufacturer had no duty under tort theories of negligence or products liability to avoid causing "purely economic loss."[206]

In most states that have considered the question, cases of intentional fraud are regarded as exceptions to the economic loss rule, so long as the claim states a true action for fraud, as contrasted to a claim re-labeled in the language of fraud, but actually flowing from a mere breach of contract.[207] The status of claims grounded in negligence is far less clear and states following the economic loss doctrine, at least outside areas of established professional liability or malpractice claims.

The *Restatement* provisions on negligent misrepresentation expressly apply that theory to situations involving pure economic loss.[208] In states that fully adopt this *Restatement* rule, the tort of negligent misrepresentation is regarded as an exception to economic loss limitations. The exception is grounded in concepts about the effect of reliance and the implied assurances needed in information-based transactions. The difference between these claims and economic loss claims grounded in contract theories, however, provides one motivation for the common ruling

---

[202] *See, e.g.*, Christopher Scott D'Angelo, "The Economic Loss Doctrine, Saving Contract Warranty Law From Drowning in a Sea of Torts," 26 U. Tol. L. Rev. 591, 598 (Spring, 1995); *Fireman's Fund Ins. v. SEC Donohue, Inc.*, 679 N.E.2d 1197, 1199-1200 (Ill. 1997) ("[a] plaintiff seeking to recover purely economic losses . . . cannot recover in tort, regardless of the plaintiff's inability to recover under an action in contract.") (quoting *Anderson Elec. v. Ledbetter Erection Corp.,* 503 N.E.2d 246, 249 (Ill. 1986)); *New York State Elec. & Gas Co. v. Westinghouse Elec. Corp.,* 564 A.2d 919 (Pa. Super. Ct. 1989); *but see Auto-Owners Ins. Co. v. Chrysler Corp.*, 341 N.W.2d 223 (Mich. Ct. App. 1983); *Sunnyslope Grading, Inc. v. Miller, Bradford & Risberg*, 437 N.W.2d 213 (Wis. 1989).

[203] *Seely v. White Motor Co.*, 403 P.2d 145, 150 (Cal. 1965).

[204] *Seely v. White Motor Co.*, 403 P.2d 145, 151 (Cal. 1965).

[205] *East River Steamship Corp. v. Transamerica Delaval, Inc.,* 106 S. Ct. 2295, 2296-97 (1986).

[206] *East River Steamship Corp. v. Transamerica Delaval, Inc.,* 106 S. Ct. 2295, 2304 (1986).

[207] See, e.g. *Huron Tool & Engineering Co. v. Precision Consulting Services, Inc*., 532 N.W.2d 541, Mich. App. (1995); NIMMER, INFORMATION LAW, ¶10.16 at 10-65.

[208] RESTATEMENT (SECOND) OF TORTS § 552(1)(2).

in courts that establishing a claim for negligent misrepresentation requires proof of a "special relationship." The relationship takes the claim out of the economic loss theory.[209]

Many courts have expanded the economic loss doctrine to tort actions for negligent misrepresentation, particularly in professional liability cases involving accountants and attorneys,[210] based on a determination that the economic loss doctrine applies to services as well as goods.[211] These courts have applied the definition of the Restatement (Second) of Torts § 552 in analyzing the question of whether the tort of negligent misrepresentation is an exception to the economic loss doctrine, since negligent misrepresentation cases generally involve third parties outside the contractual relationship, making tort recovery perhaps the plaintiff's only available remedy. New York has taken an intermediate approach, similar to its position regarding professionals generally, which allows tort actions for negligent misrepresentation even for purely economic losses between parties with a relationship "so close as to approach that of [contractual] privity."[212]

Because of the financial nature of the losses that would be suffered by users of certificates improperly issued by the CA, the CA may be protected from third party tort actions for economic losses in states which preclude recovery in tort for purely economic losses based on negligent misrepresentation.[213] But in states where negligent misrepresentations to third parties is an exception to the economic loss doctrine,[214] such as Illinois, CAs closely fit the Section 552 definition used by the courts for those liable for negligent misrepresentation. In Illinois particularly, CAs would appear to be open to tort liability under the Illinois Supreme Court's *Moorman* decision doctrine, which has a specific exception from the protection of the economic loss rule in actions for damages caused "where one who is in the business of supplying information for the guidance of others in their business transactions makes negligent representations."[215]

---

[209] NIMMER, INFORMATION LAW ¶10.16 at 10-65.

[210] *See* Reeder R. Fox and Patrick J. Loftus, "Riding the Choppy Waters of East River: Economic Loss Doctrine Ten Years Later," 64 Def. Couns. J. 260, 267 & n.66 (April, 1997) (citing cases regarding negligent misrepresentation and the economic loss doctrine).

[211] Reeder R. Fox and Patrick J. Loftus, "Riding the Choppy Waters of East River: Economic Loss Doctrine Ten Years Later," 64 Def. Couns. J. 260, 267 & nn.53-56 (April, 1997).

[212] *Credit Alliance Corp. v. Arthur Andersen & Co.*, 483 N.E.2d 110 (N.Y. 1985), *amended on other grounds*, 489 N.E.2d 249 (N.Y. 1985).

[213] These states include, for example, Pennsylvania, *Duquesne Light Co. v. Westinghouse Elec. Corp.*, 66 F.3d 604, 620 (3d Cir. 1995) (applying Pennsylvania law), *Bailey Farms Inc. v. Nor-Am Chem. Co.*, 27 F.3d 188, 192 (6th Cir. 1994), Arizona, *Apollo Group, Inc. v. Avnet, Inc.*, 58 F.3d 477, 479 (9th Cir. 1995), Florida, *see Audiotext Communications Network, Inc. v. U.S. Telecom Inc.*, 912 F. Supp. 469, 474 (D. Kan. 1995) (applying Florida law), Kansas, *Ritchie Enter. v. Honeywell Bull, Inc.*, 730 F. Supp. 1041, 1052 (D. Kan. 1990), and South Carolina, *Bishiop Logging Co. v. John Deere Indus. Equip. Co.*, 455 S.E.2d 183 (S.C. App. 1995).

[214] These states include Hawaii, *Bronster v. U.S. Steel Corp.*, 919 P.2d 294 (Hawai'i 1996), Illinois, *Fireman's Fund Ins. v. SEC Donohue, Inc.*, 679 N.E.2d 1197, 1199-1200 (Ill. 1997), and West Virginia, *In re Ford Motor Co. Bronco II Product Liab. Litig.*, 1995 U.S. Dist. Lexis 18207 (E. D. La. Dec. 4, 1995) (applying West Virginia law).

[215] *Moorman Mfg. Co. v. National Tank Co.*, 435 N.E.2d 443, 448, 452 (Ill. 1982); *see also Fireman's Fund Ins. v. SEC Donohue, Inc.*, 679 N.E.2d 1197, 1199-1200 (Ill. 1997).

This exception, and the concept of information suppliers, is construed narrowly by the Illinois courts to focus on "the ultimate result of the professional's work" in concluding whether the act of supplying information is material or ancillary to the transaction.[216] Under this analysis, attorneys,[217] real estate brokers,[218] and accountants[219] have had tort actions proceed against them for economic losses based on a claim of negligent misrepresentation, but architects,[220] engineers,[221] and those selling their home[222] have been found exempt from such actions under the economic loss doctrine and *Moorman* exceptions. As one justice pointed out in dissent, these case-by-case results "[fail] to coherently differentiate between these professional groups," and therefore "[place] trial judges and litigants in the unenviable position of guessing which additional professionals will receive protection under *Moorman's* economic loss doctrine."[223]

4.6 Controlling Reasonable Reliance through Notices and Disclaimers

Some legal support may be found for the proposition that a CA should be able to define or limit the scope of the certificate it issues, thus precluding third parties from justifiably relying on the certificate beyond that defined scope. Particularly, a small number of cases dealing with the liability of accountants and financial publishers hold or suggest that information providers may be able to limit their potential liability to third parties for negligent misrepresentation by disclaiming any reliance on the information they issue or by limiting reliance to certain specific persons or groups. By using disclaimers to define the scope of the product or services they provide, information providers may be putting third parties on notice that any reliance on the information contrary to the disclaimer may be unreasonable and thus may be undertaken at the relying party's own risk.

Thus, while contract disclaimer terms will not necessarily overcome liability for intentional fraud, they can control questions about justifiable reliance and, in appropriate cases,

---

[216] *Fireman's Fund Ins. v. SEC Donohue, Inc.*, 679 N.E.2d 1197, 1201 (Ill. 1997).

[217] *See, e.g., Fireman's Fund Ins. v. SEC Donohue, Inc.*, 679 N.E.2d 1197, 1202 (Ill. 1997) (Heiple, J., dissenting) ("The majority . . . has seen fit to continue a piecemeal approach [to the economic loss doctrine] by applying the Moorman doctrine to professional malpractice of architects and now engineers but not to attorneys or accountants.").

[218] *Zimmerman v. Northfield Real Estate, Inc.*, 510 N.E.2d 409, 415 (Ill. App. 1 Dist. 1986) (holding that realtors are "in the business of supplying . . . information" for the guidance of others in their business transactions).

[219] Illinois accountants have been excepted out of negligent misrepresentation liability by statute, and may only face liability for intentional or fraudulent misrepresentations. 225 ILL. COMP. STAT. ANN. 450/30.1 (West 1997).

[220] *See Fireman's Fund Ins. v. SEC Donohue, Inc.*, 679 N.E.2d 1197, 1200-01 (Ill. 1997) (citing *2314 Lincoln Park West Condominium Ass'n v. Mann, Gin, Ebel & Frazier, Ltd.*, 555 N.E.2d 346 (Ill. 1990)) ("In *2314 Lincoln Park West*, this court held that the economic loss doctrine applied to architects, preventing the recovery of purely economic losses in tort.").

[221] *Fireman's Fund Ins. v. SEC Donohue, Inc.*, 679 N.E.2d 1197, 1201 (Ill. 1997) ("We hold that the economic loss doctrine bars recovery in tort against engineers for purely economic losses.").

[222] *Zimmerman v. Northfield Real Estate*, 510 N.E.2d 409, 415 (Ill. 1986). However, the persons selling their home in this case were found liable of intentional misrepresentations, which is not an exception to the economic loss doctrine. *Id.*

[223] *Fireman's Fund Ins. v. SEC Donohue, Inc.*, 679 N.E.2d 1197, 1202 (Ill. 1997) (Heiple, J., dissenting).

define the terms of the intended scope of reliance.[224] The efficacy of a disclaimer or a statement restricting reliance on the information to designated parties depends in part on the specificity of the terms and their resulting impact on actual or reasonable reliance or on defining the scope of the information provider's intended undertaking.[225] A conspicuous statement indicating that information is not to be used for certain purposes may exclude negligent misrepresentation liability under the *Restatement*. A similar disclaimer about the accuracy or inaccuracy of the information should likewise control and preclude such claims.[226]

4.6.1 Accountants' Opinion Letter Disclaimers

Some courts have held or suggested that an accountant may be able to limit third party reliance on its opinion letter by including in the letter an express disclaimer that third parties, or third parties not falling within a defined group, should not rely on the opinion. Because reasonable reliance on the information must be shown in a negligent misrepresentation case,[227] the general effect of such a disclaimer may be to put third parties on notice that any reliance on the opinion letter contrary to the disclaimer may be deemed unreasonable and thus may preclude them from recovery in the event that errors occur in connection with the issuance of the opinion.

In *First National Bank v. Sparkmon* a Georgia court held that disclaimers contained in an accountants' review report and various compilation reports were "effective to preclude any justifiable reliance by a third party upon the review and compilation reports they prefaced."[228] The disclaimer contained in the review report warned that the review was substantially less in scope than an audit and that the accountants did not express an opinion on the accuracy of the financial reports. Similarly, the compilation reports warned that the accountants did not express an opinion or other assurance regarding the financial statements, and emphasized that the client had omitted substantially all of the disclosures ordinarily included in financial statements. The court reasoned that the accountants' duty to third persons could be "limited by appropriate

---

[224] Nimmer, information law at ¶10.17 at 10-66.

[225] Compare *Paracor Financing Inc. v. General Electric Capital Corp.,* 79 F.3d 878, 9th Cir. (1996) (investors could not justifiably rely on representations by financier of leveraged buy-out because they signed an agreement saying they made their decision to purchase "without relying on any other person") and *J/H Real Estate, Inc. v. Abramson*, 901 F.Supp. 952, E.D. PA (1995) (cautionary statements did not render misrepresentations and omissions in material).

[226] NIMMER, INFORMATION LAW at ¶10.17 at 10-67.

[227] *See, e.g., Rosenstein v. Standard and Poor's Corp.,* 636 N.E.2d 665, 669 (Ill. App. Ct. 1993) (stating "we have required that the plaintiff reasonably rely upon the information conveyed by the defendant"). See also, RESTATEMENT (SECOND) OF TORTS § 552 (1977).

[228] 442 S.E.2d 804, 805 (Ga. Ct. App. 1994), *cert. denied* (Jul. 07, 1994). For an earlier Georgia case giving effect to accountants' disclaimers, *see MacNerland v. Barnes,* 199 S.E.2d 564 (Ga. Ct. App. 1973) (holding accountants are not liable to third parties for negligence in preparing and issuing uncertified financial statements that contain an express disclaimer of opinion even though third party reliance on the financial statements is known or could be anticipated). *But see ML-Lee Acquisition Fund, L.P. v. Deloitte & Touche,* 463 S.E.2d 618, 634-35 (S.C. Ct. App. 1995), *reh'g denied* (Nov. 17, 1995), *cert. granted* (Aug. 22, 1996), *aff'd in part, rev'd in part on other grounds,* 489 S.E.2d 470 (S.C. 1997) (stating that limited scope of comfort letter and inclusion of disclaimer does not require finding that reliance on letter was not justified as matter of law, but rather whether reliance was justifiable is a question of fact).

disclaimers which would alert those not in privity with the supplier of information that they may rely upon it only at their peril."[229] The court implied that this is true notwithstanding that the third persons were foreseeable or that the information was intended to reach them.[230]

In *Stephens Industries, Inc. v. Haskins and Sells* a public accounting firm was held not liable to an investor who relied on the accountants' audit reports in purchasing stock in the subject companies where the accountants were instructed by the companies not to audit the accounts receivable and the audit reports expressly reflected these instructions.[231] Among the factors contributing to the court's decision was the fact that the accountants "followed the scope of audit as outlined by their clients, and carefully limited their work product results to coincide exactly with the undertaking."[232]

In *Evans v. Israeloff, Trattner & Co.* a New York court granted summary judgment for and dismissed a complaint for fraud against accountants who had issued monthly compilation reports containing misrepresentations as to the company's financial health.[233] The court ruled that the investor could not claim justifiable reliance on the alleged misrepresentations where, among other things, each compilation report was accompanied by a cover letter containing a disclaimer that included the following language:

> A compilation is limited to presenting in the form of financial statements information that is the representation of management. We have not audited or reviewed the accompanying financial statements and, accordingly, do not express an opinion or any other form of assurance on them.[234]

Other courts have suggested in dicta that a disclaimer might be used to help reduce the potential for liability for negligent misrepresentation.[235]

---

[229] 442 S.E.2d at 805 (citing *Robert & Co. Assoc. v. Rhodes-Haverty Partnership,* 300 S.E.2d 503 (Ga. 1983)).

[230] *See id.*

[231] 438 F.2d 357 (10th Cir. 1971) (applying Colorado law).

[232] *Id.* at 361. Among the other factors contributing to the court's decision was the fact that the investor agreed to the scope of the accountants' audit as evidenced by the purchase agreement it entered into with the subject companies.

[233] 617 N.Y.S.2d 899 (N.Y. App. Div. 1994), *appeal denied,* 655 N.E.2d 401 (N.Y. 1995).

[234] Id. at 900.

[235] *See, e.g., H. Rosenblum, Inc. v. Adler,* 461 A.2d 138, 152 (N.J. 1983) ("The auditors could in some circumstances, such as when auditing a privately owned company, expressly limit in their certificates the persons or class of persons who would be entitled to rely upon the audit."); *Fleet Nat'l Bank v. The Glouster Corp.,* No. 92-11812-REK, 1994 U.S. Dist. LEXIS 21055, at *33-36 (D. Mass. August 8, 1994) ("the key [to meeting the needs of the accountant's clients while protecting the reasonable expectations of third parties] is to permit the auditor to put an appropriate disclaimer in the audit opinion itself, identifying those persons who are or are not entitled to rely upon that opinion"; such an express disclaimer might preclude a finding that a third party's reliance was reasonable). *See also Bily v. Arthur Young & Co.,* 834 P.2d 745, 785-86 (Ca. 1992) (Kennard, J., dissenting) ("[liability] disclaimers give fair notice to all potential report users and prevent third parties' reliance from being reasonable").

Although the situation of a CA issuing certificates in some ways would appear to be analogous to that of a public accountant issuing an opinion letter, whether a court would extend the applicability of disclaimers to a CA remains uncertain. Furthermore, as discussed in more detail below, the requirement of adequate notice may pose an obstacle to a CA's ability to use a disclaimer. Unlike an accountant's opinion letter which easily can accommodate a conspicuous disclaimer, certificates are not nearly as flexible. Moreover, unlike an opinion letter which can disclaim reliance on the face of the document itself, a certificate may only be able to incorporate the disclaimer by reference.

4.6.2 Financial Publishers' Disclaimers

Certain cases involving negligent misrepresentation as to publishers of financial information also suggest that information providers may be able to expressly disclaim reliance by third parties on the information they issue.

In *Gale v. Value Line, Inc.,* the publisher of a periodical that ranked convertible securities and included purchase recommendations was sued for negligent misrepresentation when it failed to include information regarding the expiration of certain warrants that, if included, may have prevented certain losses incurred by a reader.[236] The front page of each edition of the publication contained a disclaimer that read: "Factual material is obtained from sources believed to be reliable but cannot be guaranteed." The reader argued that the purpose of this disclaimer was to protect the publisher from the errors of others but did not apply to errors made by the publisher itself. The court, agreeing with the reader's interpretation, suggested that:

> Had the [publisher] wished to protect itself from its own errors as occurred in this instance, it could have said it so much more clearly, for example: "The publisher is not responsible for any errors or omissions." Contrasted in this light, the so-called disclaimer is not adequate to insulate the defendant from liability.[237]

The court's language suggests that information providers might be able to limit their potential liability to third parties by disclaiming reliance on the information. However, because the court merely expressed this theory in dicta and did not rely on it in deciding the case, its practical applicability remains uncertain.

One means of attempting to increase the possibility that an exculpatory clause will be given effect is to require the party with whom the information provider is in contractual privity (i.e., subscribers in the case of a CA) to incorporate the exculpatory clause into its agreements with third parties (i.e., relying parties). At least one court has recognized this as an effective means of disclaiming liability. Specifically, the court gave effect to an exculpatory clause contained in a license agreement between a provider of securities closing price indexes and a securities exchange that stated:

---

[236] 640 F. Supp. 967 (D.R.I. 1986).

[237] 640 F. Supp. at 970.

> S & P shall obtain information for inclusion in or for use in the calculation of the S & P Indexes from sources which S & P considers reliable, but S & P does not guarantee the accuracy and/or the completeness of any of the S & P Indexes or any data included therein. S & P MAKES NO WARRANTY, EXPRESS OR IMPLIED, AS TO RESULTS TO BE OBTAINED BY ANY PERSON OR ANY ENTITY FROM THE USE OF THE S & P INDEXES OR ANY DATA INCLUDED THEREIN IN CONNECTION WITH THE TRADING OF THE CONTRACTS, OR FOR ANY OTHER USE. S & P MAKES NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE FOR USE WITH RESPECT TO THE S & P INDEXES OR ANY DATA INCLUDED THEREIN. [Exchange] Rules shall expressly include the disclaimer language contained in this Paragraph"[238]

The information provided by Standard & Poor's (S & P) in the form of its S & P Indexes was used by the Chicago Board Options Exchange (Exchange) to establish the sale price of option contracts. When S & P incorporated erroneous closing prices into its S & P Indexes it was sued for negligent misrepresentation by a securities options trader who suffered losses when the option contracts he sold were valued incorrectly based on the information provided to the Exchange by S & P.

Central to the court's finding that the clause expressly exculpated S & P from liability to the options trader was the fact that the clause was incorporated into the rules of the Exchange to which the options trader's transactions were subject. Thus in this case the information provider went beyond merely disclaiming any reliance by third parties and instead took measures to expressly bind third parties to the disclaimer through contract. The court admonished that: "While such exculpatory clauses may not be favored and are strictly construed against the benefiting party, there is a broad public policy permitting competent parties to contractually limit their respective liability and to allocate business risks in accordance with their business judgment."[239]

This case suggests that CAs may be able to contractually bind third parties to exculpatory clauses by requiring subscribers to incorporate such provisions in their respective contracts with third parties. Short of this, however, it remains unclear whether CAs could rely merely on a disclaimer to limit their potential liability to third parties for negligent misrepresentation liability.

4.6.3 Adequate Notice

Assuming for purposes of this discussion that a disclaimer by a CA may be given effect, the issue then becomes one of notice. Given the limited space on a certificate to set forth a disclaimer, and given that in some instances a relying party may not even see the certificate itself, concern arises as to how a CA might provide relying parties adequate notice of the

---

[238] *Rosenstein v. Standard and Poor's Corp.,* 636 N.E.2d 665, 666-67 (Ill. App. Ct. 1993) (emphasis in original).

[239] 636 N.E.2d at 671. Note that the options trader failed to plead that S & P did not promptly correct the inaccuracy as required by the license agreement. It is unclear whether this claim, if pleaded, would have affected the court's ruling.

disclaimer. Given the unique nature of the relationship between a CA and relying parties, and the unique nature of the services that a CA provides, cases pertaining to adequacy of notice are not easily analogized. Thus the general discussion of the law pertaining to notice which follows provides only very limited guidance for CAs.

The term "notice" has various meanings, and the question of whether a party has been given notice depends largely on the context. "Notice" in its legal sense may be defined generally as:

> [I]nformation concerning a fact actually communicated to a person by an authorized person, or actually derived by him from a proper source, or else presumed by law to have been acquired by him, which information is regarded as equivalent in its legal effects to full knowledge of the fact, and to which the law attributes the same consequences as would be imputed to knowledge. In its full legal sense, the term embraces a knowledge of circumstances that ought to induce suspicion or belief or put a prudent person on inquiry, as well as direct information of the fact.[240]

Notice can be either "actual" or "constructive," and "actual notice" can be either "express" or "implied." Constructive notice differs from actual notice in that it constitutes neither notice nor knowledge as such, but rather it is a fiction that is imposed by law for reasons based on public policy.[241] A typical example of constructive notice is notice which is imputed by reason of a title recording statute. Actual notice, on the other hand, arises from inferences of fact.[242] Because only actual notice can be affirmatively given by a party (rather than inferred by law), it is that subject to which we turn.

(a) Express Notice

"Actual notice" may be either express or implied.[243] "Express notice" is that which is actually "brought home" to the party directly.[244] This is often accomplished by communicating information directly to the person to whom notice is to be given and can be either written or oral.[245]

A CA, for example, might provide express notice of a disclaimer by communicating that information directly to relying parties. Given the "physical" limitations of a certificate, however, it is unlikely that such direct communication could be accomplished easily. There is very little space available on a certificate to set forth a disclaimer in its entirety. And in situations where the certificate is handled automatically by the relying party's software, the certificate and any

---

[240] 66 C.J.S. *Notice* § 2 (1950) (footnotes omitted).

[241] 66 C.J.S. *Notice* § 6 (1950).

[242] 66 C.J.S. *Notice* § 7 (1950).

[243] Black's Law Dictionary 1061 (6th ed. 1990).

[244] 66 C.J.S. *Notice* § 4 (1950).

[245] *See* 66 C.J.S. *Notice* § 4 (1950).

disclaimers contained therein may not even been seen by the relying party. Thus a CA is likely find itself in the position of having to rely on a less direct or "implied" means of notice.

(b) Implied Notice

Recognizing that the "physical" limitations of a certificate may prevent a CA's entire disclaimer from appearing on the face of the certificate itself, a question arises as to whether a brief statement in the certificate directing the relying party to inquire in the CAs CPS is sufficient to put the relying party on notice as to the entire contents of the disclaimer. In other words, by virtue of making some information directly known to the relying party, can notice of all of the related information be implied? The lack of analogous case law causes this question to remain unanswered.

This concept of "incorporation by reference" has been debated at length at the UNCITRAL meetings. Some countries have indicated that the concept violates fundamental principles of their laws, whereas other countries (including the U.S.) have focused more on aspects of notice, accessibility, availability, and consumer protection. At the recently completed UNCITRAL meeting, the group agreed to include an incorporation by reference provision in the Model Legislation that would simply state that a contract term or notice shall not be deemed ineffective "solely" because it is incorporated by reference. That leaves it to applicable law (which is, of course, not clear) as to whether the incorporation by reference actually becomes effective. However, the following general discussion of the law pertaining to implied notice may provide some very limited guidance.

"Implied notice" may be distinguished from express notice in that the knowledge imputed to the receiving party is not directly communicated in its entirety to the receiving party. But like express notice, implied notice is the equivalent of actual notice because if the information made known to the receiving party is sufficient to put that person on inquiry, it need not constitute the whole of the information of which knowledge will be imputed.[246] Implied notice is "inferred or imputed to a party by reason of his knowledge of facts or circumstances collateral to the main fact, of such a character as to put him upon inquiry, and which, if the inquiry were followed upon with due diligence, would lead him definitely to the knowledge of the main fact."[247] Implied notice, therefore, is a presumption of knowledge of the ultimate facts that arises when a party has actual knowledge of circumstances sufficient to enable that party, through reasonable inquiry, to learn of the ultimate facts.[248]

Actual notice will be implied, however, only "when the known facts are sufficiently specific to impose the duty to investigate further and when such facts furnish a natural clue to the ultimate fact."[249] Moreover, a person put on inquiry must be given a reasonable time to make such inquiry before being imputed with notice.[250]

---

[246] 66 C.J.S. *Notice* §§ 5, 11(b)(4)(a) (1950).

[247] Black's Law Dictionary 1062 (6th ed. 1990).

[248] *See* 66 C.J.S. *Notice* § 5 (1950); Black's Law Dictionary 1062 (6th ed. 1990).

[249] 66 C.J.S. *Notice* § 5 (1950).

[250] 66 C.J.S. *Notice* § 11(b)(3) (1950).

(1) Sufficiency of Facts to Impose Duty to Inquire

There is no set rule to determine what constitutes sufficient facts to put a person on inquiry -- each case depends on its own facts and circumstances.[251] However, it can be said that the facts made known to the party must be sufficient to excite inquiry in light of circumstances.[252] The information with respect to which notice is to be imputed must be naturally and reasonably connected with the facts known to the party such that the known facts can be said to furnish a clue.[253] Moreover, the means of gaining knowledge of the information with respect to which notice is to be imputed "must be available and of such a character that a prudent man might be expected to take advantage of them."[254]

(2) Reasonable Time to Inquire

A person put on inquiry must be given reasonable time to make such inquiry before being imputed with notice.[255] What constitutes reasonable time depends on the facts and circumstances of each case.[256]

---

[251] 66 C.J.S. *Notice* § 11(b)(4)(a) (1950).

[252] *See, generally,* 66 C.J.S. *Notice* § 11(b)(4) (1950).

[253] See 66 C.J.S. *Notice* § 11(b)(4)(b) (1950).

[254] *See* 66 C.J.S. *Notice* § 11(b)(4)(a) (1950).

[255] 66 C.J.S. *Notice* § 11(b)(3) (1950).

[256] 66 C.J.S. *Notice* § 11(b)(3) (1950).

5. CONTRACT LIABILITY

5.1 What Law Applies to a CA's Activities?

A CA's contractual and warranty obligations depend, in part, on what law applies to its certification authority activities. Article 2 of the Uniform Commercial Code ("UCC") governs transactions in goods,[257] the common law applies to transactions in services and to contracts involving more specifically the provision of information, and UCC Article 2B[258] (a revision of the UCC that could be approved within the coming year) would modernize the licensing of information.[259] If a transaction involves both the sale of goods and the provision of services, whether the UCC or common law applies depends upon the jurisdiction.

Courts may, with some justice, view the role of a CA as combining elements of providing a service and selling a good. In such "mixed" cases, courts consider the applicability of Article 2 of the UCC to be a question of fact concerning the nature of the transaction.

If the seller is providing a hybrid of a good and a service, the **majority view** applies the *predominant factor test* to determine which of the two predominates the transaction.[260] In jurisdictions taking the majority view, a court will ask: "What is the essence or main objective of the parties' agreement?" or "What is the purchaser's ultimate goal?" If the goods component predominates, the court will apply the UCC to the entire transaction. If the services component predominates, the court will apply common law to the entire transaction.[261]

The **minority view** applies the UCC to the goods component of the transaction and the common law to the services component.[262] CAs may be able to manipulate this characterization in some jurisdictions. For example, a CA that gives a client a certificate may more likely be considered to be selling a "good" than a CA that enters into a "service contract" by which the CA agrees to make the certificate available on a web page to all who wish to see it.

---

[257] *See* UCC § 2-102.

[258] National Conference of Commissioners on Uniform State Laws, UCC Article 2B (February 1998 draft).

[259] This memorandum focuses on UCC Article 2 and, to a lesser extent, proposed Article 2B, and does not consider other UCC sections that have a remote chance of applying to CA activities (and thus beyond the scope of this memorandum). For example, as a mere confirmation of identity, a digital certificate probably is not a "document of title" under UCC Article 3, but it can potentially play other roles -- such as serving as a transaction document (CA serves as witness) or operating in a time-stamping function -- that could arguably raise issues covered by Article 3, which governs negotiable instruments, fictitious payees, imposters, and the like.

[260] *See, e.g., Neibarger v. Universal Co-Operatives, Inc.,* 486 N.W.2d 612 (Mich. 1992); *St. Ann-Nackawic Pulp Co. v. Research-Cottrell, Inc.,* 788 F. Supp. 729 (S.D.N.Y. 1992).

[261] *Corporate Counsel's Guide to the Uniform Commercial Code* at 2.001-.002 (1993).

[262] A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce,* 75 Or. L. Rev. 49, 89 (Spring 1996).

Still **other states** either use a *final product test*, which looks at what is left when a contract is completed[263] or attempt to determine which classification best serves public policy.[264] Because the courts have failed to achieve anything approaching uniformity in how they characterize the facts in mundane transactions, it is entirely possible that courts in different jurisdictions will disagree about how best to characterize a CA's provision of certificates in the absence of legislation.

Thus, under contract law, we must consider all the activities in which a CA may engage (either directly or via a third part CMA) and attempt to classify them as involving goods, services, or both. Under proposed Article 2B, we should also consider whether any of these activities involve "information." These activities may include:

- authenticating subscribers by:
  - ✓ verifying identity, and
  - ✓ binding a subscriber to a key pair;
- issuing certificates through a CMA;
- receiving and transmitting certificates;
- revoking and suspending certificates;
- maintaining a repository and a CRL; and
- managing certificates (e.g., storage and access control via a repository);

For purposes of this memorandum, we are assuming that a CA could engage in each of these activities.

A CA's activities in receiving, transmitting, revoking, suspending, and managing certificates appear to be classic examples of services, as do a CA's activities in maintaining a repository and CRL. In general, activities such as data processing services, including computerized data analysis, collection, storage, and reporting, are generally not treated as goods and are not subject to the UCC.[265]

A CA's activities in authenticating subscribers arguably could constitute a provision of either goods or services. If a subscriber's (or relying party's) goal is to obtain reliable identification of someone and to bind that person to a key pair, even if those services are memorialized in a certificate, then arguably the activities represent a service. Merely because information or the product of a service is reduced to a report or is otherwise stored on some

---

[263] Crystal A. Miller, Note, *The Goods/Service Dichotomy and the U.C.C.: Unweaving the Tangled Web,* 59 Notre Dame L. Rev. 717, 726 (1984).

[264] Crystal A. Miller, Note, *The Goods/Service Dichotomy and the U.C.C.: Unweaving the Tangled Web,* 59 Notre Dame L. Rev. 717, 728-29 (1984).

[265] *See, e.g., Computer Servicenters, Inc. v. Beacon Mfg. Co.*, 328 F. Supp. 653, 655 (D. S.C. 1970), *aff'd,* 443 F.2d 906 (4th Cir. 1971) (contract for performance of data processing services is not "sale of goods"); *Data Processing Servs., Inc. v. L.H. Smith Oil Corp*., 492 N.E.2d 314 (Ind. Ct. App. 4 Dist. 1986); *but see Hospital Computer Sys., Inc. v. Staten Island Hosp*., 788 F. Supp. 1351 (D. N.J. 1992) (data processing contract involving a sale of software modified for the client's data processing needs held to be a sale); *Colonial Life Ins. Co. v. Electronic Data Sys. Corp*., 817 F. Supp. 235 (D. N.H. 1993) (contract providing for over four years of data processing and software development services was a transaction in goods within Article 2 under New Hampshire law).

physical medium does not change the underlying nature of the transaction. For example, courts have found the services component of each of the following transactions to predominate:

- contract to manufacture release prints of a motion picture and to deliver those for exhibition was predominantly a services transaction because the essence of the contract was to provide services and the transfer of personal property was only incidental;[266]
- contract for a real estate survey was predominantly a services transaction because the survey did not constitute "goods" and the goal was the rendition of services;[267]
- contract for the design of a brochure was predominantly a services transaction, and the physical layout of the brochure was not a good;[268]
- contract for printing and production of children's books was predominantly a services transaction even though the printer supplied the materials for the books.[269]

If, however, the goal is to obtain a certificate, then arguably, the activities could be deemed to be provision of a good.[270]

A CA's activities as a whole can be characterized as "mixed" in that they are likely to involve both goods and services components. In a minority jurisdiction, the CA must consider its liability for the goods component of its activities under the UCC and for the services component under common law. In a majority jurisdiction, it is not clear whether a court would conclude that the services or the goods component of the activities predominate. The analysis is highly fact-sensitive, and it is difficult to predict the outcome in any given case. Moreover, because the CA would arguably be acting as an information provider in its CA activities, the common law governing information providers and the new UCC Article 2B proposed statutory language must also be considered in assessing the CA 's potential liability.

The official Reporter's Notes for proposed Article 2B recognize the implications of the three legal traditions on the law of warranty:

> Article 2B warranties blend three different legal traditions. **One** tradition stems from the UCC and focuses on the quality of the product. This tradition centers on the result delivered: a product that conforms to ordinary standards of performance.
>
> The **second** tradition stems from common law, including cases on licenses, service contracts and information contracts. This tradition focuses on how a contract is performed, the process rather than the result. The obligations of the transferor are to perform in a reasonably careful and workmanlike manner.

---

[266] *Filmservice Labs., Inc. v. Harvey Bernhard Enter., Inc.,* 208 Cal. App. 3d 1297 (Cal. Ct. App. 2 Dist. 1989).

[267] *Raffel v. Perley*, 437 N.E.2d 1082 (Mass. Ct. App. 1982).

[268] *Incomm v. Thermo-Spa*, 595 A.2d 954 (Conn. Super. 1991).

[269] *For Children, Inc. v. Graphics Int'l, Inc*., 352 F. Supp. 1280 (S.D.N.Y. 1972).

[270] *Lake Wales Publishing Co. v. Florida Visitor*, 355 So.2d 335 (Fla. App. 1976) (contract for compiling, editing, and publishing pamphlets is transaction in goods).

The **third** tradition comes from the area of contracts dealing with informational content and essentially disallows implied obligations of accuracy or otherwise in reference to information transferred outside of a special relationship of reliance.

Current law selects the appropriate tradition based in part on characterizations about whether a transaction involves goods or not. That distinction is not reliable in information contracting, especially in light of the ability to transfer information electronically without the use of any tangible property to carry the intangibles.[271]

As the discussion below on exculpatory clauses and disclaimers indicates, these legal traditions -- and the potential applicability of the proposed Article 2B (which is geared toward software and information contracts) -- will affect the CA's ability to limit both warranties and liability.

5.2 Warranties Arising Under the UCC

Because at least some of a CA's certification authority activities could be characterized as selling or transacting in goods, or because a court could look to the UCC as highly persuasive authority even where the services component of the transaction predominates, the warranty and limitation of liability provisions of Article 2 of the UCC must be considered in assessing the CA's potential liability under a contract theory.[272]

In analyzing the applicability of the UCC warranty provisions, two key questions must always be considered: (1) What warranties apply? and (2) Who receives the benefit of the warranties?

Key to determining the answers to these questions are the three types of contractual relationships that could arise in the context of the CA's certification activities. These include:

- The CA's agreements with its subscribers;
- The CA's agreement with a CMA; and
- Agreements (if any) between the CA and relying parties.

With respect to each contract, three types of warranties could arise under Article 2 or 2B of the UCC: (1) express warranties, (2) implied warranties of merchantability (including Article 2B's new implied warranty with regard to information content), and (3) implied warranties of fitness for a particular purpose.[273] In addition, Section 2-318 of the UCC extends all sales

---

[271] National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 403, Reporter's Note 1 (February 1998 draft).

[272] *See also* National Conference of Commissioners on Uniform State Laws, UCC Article 2B §§ 401 - 409 (February 1998 draft), which also provides warranties that could apply to the CA's activities.

[273] A fourth type of warranty, a warranty of title and against infringement (UCC § 2-312), could theoretically apply to the extent that the goods that the CA is providing have intellectual property attributes; because the possibility of this seems remote, we do not address it in this memorandum. In any case, such warranties can be disclaimed under UCC § 2-312(2), which requires either specific language or certain circumstances that put the buyer on notice.

warranties arising under the UCC -- whether express or implied -- to certain persons other than the purchaser on the theory that such persons are third-party beneficiaries of the warranties. Similar warranties to third-party beneficiaries could also arise under proposed Article 2B.[274]

5.2.1 Express Warranties

Under Section 2-313 of the UCC (and Section 402 of Article 2B), express warranties can arise in a number of ways. First, *any affirmation of fact* or *promise* made by the CA that relates to the goods (i.e., the certificates) and becomes part of the basis of the bargain creates an express warranty that the goods shall conform to the affirmation or promise.[275] For example, statements in a CPS could constitute a warranty.

Second, *any description of the goods* that is made part of the basis of the bargain creates an express warranty that the goods shall conform to the description.[276] For example, the CA's representation that it will use the X.509 version 3 certificate format could constitute a description of the goods that becomes a part of the basis of the bargain. By representing that it will use the X.509 version 3 format, the CA will be creating an express warranty that the certificates it provides shall conform to the description of this format.[277] Likewise, by representing that it will issue a certificate, the CA will be creating an express warranty that, at a minimum, it will be following a procedure that will provide certificates that contain the subscriber's name, the subscriber's public key, and the CA's digital signature.

The CA can be deemed to have made an express warranty under the UCC without using formal words such as "warrant" or "guarantee" and without having any intent to make a warranty.[278] For example, statements in a CA's CPS could constitute an express warranty, as could a commitment to issue certificates in X.509 version 3 format. On the other hand, a CA will not create a warranty under the UCC simply by affirming the value of, or commending, the certificate.[279] A seller can generally give its opinion of goods, i.e. puffing, without creating an express warranty. The line between promising and puffing, however, can often be hard to draw. For example, despite a defendant's attempts to characterize as puffing a memo to its distributors regarding the extensive testing and intense investigation of a new carburetor it had developed, the Eleventh Circuit held that the defendant had a duty at the very least to obtain knowledge of the memo's truth before uttering the representation.[280] The key question is: "[w]hat statements

---

[274] *See* National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 409 (February 1998 draft).

[275] UCC § 2-313(1).

[276] UCC § 2-313(1).

[277] Any *sample or model* that is made part of the basis of the bargain also creates an express warranty that the whole of the goods shall conform to the sample or model (UCC § 2-313(1)), but this basis for an express warranty is unlikely to apply to the CA and thus is not considered here.

[278] UCC § 2-313(2).

[279] UCC § 2-313(2).

[280] *Dancey Co., Inc. v. Borg-Warner Corp.,* 799 F.2d 717, 718-720 (11th Cir. 1986). With respect to that memorandum, evidence was introduced regarding what constituted sufficient testing in the industry and what the plaintiff (one of the distributors) could thus infer from the representations made in the memorandum (that

of the seller have in the circumstances and in objective judgment become part of the basis of the bargain?"[281]

With regard to a sale of goods governed by the UCC, advertisements read by the potential plaintiff may also create an express warranty.[282] Specific and unequivocal statements, such as stating in capital letters: "completely safe ball will not hit player" or describing a sailboat as "a carefully well-equipped and very seaworthy vessel," can make explicit guarantees.[283] Even where the claim is not pleaded or submitted under the UCC, as in a suit based on improper provision of services, advertisements can create at least an *implied* warranty that work will be done in a workmanlike manner (where the plaintiff read an advertisement that stated that the defendant was skilled in the particular work involved).[284]

Proposed Article 2B specifically covers express warranties arising from advertisements by providing that "[a]ny affirmation of fact or promise made by the licensor to its licensee in any manner, *including in a medium for communication to the public such as advertising,* which relates to the information and becomes part of the basis of the bargain creates an express warranty that the information required under the agreement will conform to the affirmation or promise."[285] This provision would clarify the rule in Article 2 and expand the scope of express warranty rules in some states.[286] In the absence of a bargaining relationship between the licensor making representations and the licensee, liability for advertising statements would arise under tort or advertising rules, not under contract law.[287]

Thus, a CA will need to be careful whenever making any representations in its advertisements, marketing literature, notices, communications to subscribers, CPS, and any other communications with relying parties regarding the value of the CA's certificates and its procedures.

---

accompanied an invitation to an introductory meeting), which proclaimed "[a]fter many months of intensive investigation and extensive testing of various designs, Century is proud to introduce the most efficient and universally adaptable propane carburetor ever offered to the industry."

[281] UCC § 2-313, Official Comment 8.

[282] *Crank v. Firestone Tire & Rubber Co.,* 692 S.W.2d 397, 401 (Mo. Ct. App. 1985).

[283] *Maneely v. General Motors Corp.,* 108 F.3d 1176, 1181 (9th Cir. 1997), *citing Hauter v. Zogarts,* 14 Cal.3d 104, 109 (1975) and *Keith v. Buchanan,* 173 Cal.App.3d 13, 22 (Cal. Ct. App. 2 Dist. 1985), respectively, in distinguishing GM's visual advertisements as being set in certain surroundings and making no explicit guarantees.

[284] *Crank v. Firestone Tire & Rubber Co.,* 692 S.W.2d 397, 401 (Mo. Ct. App. 1985) (advertisement indicated that the defendant was skilled in the installation of oil filters in diesel Volkswagen Rabbits).

[285] *See* National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 402(a)(1) (February 1998 draft) (emphasis added).

[286] *See* National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 402, Reporter's Note 2 (February 1998 draft).

[287] *See* National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 402, Reporter's Note 2 (February 1998 draft).

5.2.2 Implied Warranties

Under Articles 2 and 2B of the UCC, certain implied warranties can arise unless they are expressly excluded or modified.[288] If an implied warranty does arise, and it is not disclaimed, it does not matter whether the seller knew of the defect or could not have discovered it. Although implied warranties impose strict liability, their protective value can be diminished by wholesale disclaimers, leaving the buyer only with an unconscionability argument or, if the buyer is a consumer, with some protection from federal and state consumer statutes.[289]

The two primary types of implied warranties are the implied warranty of merchantability and the implied warranty of fitness for a particular purpose. The two implied warranties are not mutually exclusive; often, both will apply to the same transaction and the same product (i.e., a digital certificate).[290] Other implied warranties may also arise from a course of dealing or usage of trade,[291] but these warranties may be excluded or modified pursuant to the general disclaimer provisions of Section 2-316 of the UCC.

A CA should be sure to exclude implied warranties to the extent it can under Article 2, proposed Article 2B, and state digital signature statutes, as well as to the extent it is commercially feasible (i.e., as more CAs enter the field, a CA's disclaimer of certain implied warranties arising from usage of the trade could put it at a competitive disadvantage if other CAs make more promises for a comparable fee).

5.2.2.1 Implied Warranty of Merchantability

In every transaction by a *merchant* who deals in goods of the kind sold, an implied warranty of merchantability arises -- i.e., that the goods are *merchantable*. To be merchantable, the goods must:

- pass without objection in the trade under the contract description;
- be of fair average quality within the description (for *fungible* goods);
- be fit for the ordinary purposes for which such goods are used;
- run, within the variations permitted by the agreement, of even kind, quality, and quantity within each unit and among all units involved;
- be adequately contained, packaged, and labeled as the agreement may require; and
- conform to the promise or affirmations of fact made on the container or label if any.[292]

---

[288] UCC § 2-314.

[289] *Employers Ins. of Wausau v. Suwannee River SPA Lines, Inc.,* 866 F.2d 752, 764, n.23 (5th Cir. 1989).

[290] *See* National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 403, Reporter's Note 3 (February 1998 draft).

[291] UCC § 2-314(3).

[292] UCC § 2-314(2).

The key test of merchantability is whether the goods "are fit for the ordinary purposes for which such goods are used."[293]

The question arises as to whether a CA qualifies as a *merchant.* A merchant is defined under the UCC as "a person who deals in goods of the kind or otherwise by his occupation holds himself out as having knowledge or skill peculiar to the practices or goods involved in the transaction, or to whom such knowledge or skill may be attributed by his employment of an agent or broker or other intermediary who by his occupation holds himself out as having such knowledge or skill."[294] Based on this, it is highly likely that a CA is a merchant.

Proposed Article 2B also contains provisions for an implied warranty of merchantability[295] as well as an implied warranty with regard to information content.[296] This latter provision specifies that unless this warranty is otherwise excluded or modified, "a merchant that provides informational content in a special relationship of reliance or that provides services within this article to collect, compile, process, or transmit informational content, *warrants to its licensee that there is no inaccuracy in the informational content caused by its failure to exercise reasonable care and workmanlike effort in its performance*."[297] As the first Reporter's Note for this Section indicates, no warranty of this type exists under current statutory law, but the terms of the warranty reflect case law on information contracts.[298] To disclaim or modify this implied warranty, language that mentions "accuracy," or words of similar import, will be sufficient.[299]

5.2.2.2 Implied Warranty of Fitness for a Particular Purpose

The implied warranty of fitness for a particular purpose arises whenever any seller (merchant or nonmerchant) at the time of contracting has reason to know: (1) the particular purpose for which the goods are required, and (2) that the buyer is relying on the seller's skill and judgment to select or furnish suitable goods.[300] The buyer need not provide the seller with actual knowledge of the particular purpose for which the goods are intended or of its reliance on the seller's skill or judgment -- it is enough if the circumstances are such that "the seller has reason to realize the purpose intended or that the reliance exists."[301] A "particular purpose"

---

[293] UCC § 2-314(2)(c), Official Comment 8.

[294] UCC § 2-104(1).

[295] National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 403 (February 1998 draft).

[296] National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 406(5) (February 1998 draft) (mentioning "quality" or "merchantability" is sufficient language).

[297] *See* National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 404(a) (February 1998 draft) (emphasis added).

[298] *See* National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 404, Reporter's Note 1 (February 1998 draft).

[299] *See* National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 406(b)(2) (February 1998 draft).

[300] UCC § 2-315.

[301] UCC § 2-315, Official Comment 1.

envisions a specific use by the buyer that is peculiar to the nature of its business, whereas the ordinary purpose for which goods are used envisions the concept of merchantability and uses that are customarily made of the goods in question.[302]

One commentator has argued that the information contained in certificate applications arguably puts a CA on notice regarding the particular purpose for which the certificate will be used.[303] For example, when ABC Bank applies for a certificate, the CA can be presumed to know the name of the subscriber and thus the likely nature of its business (some type of financial service). Furthermore, the CA knows that subscribers apply for certificates so that relying parties (those who will enter into some type of financial transaction with the bank) will be able to rely on the CA's verification of the subscriber's identity. Yet, the question arises if this really constitutes fitness for a particular purpose versus fitness for the ordinary purpose for which certificates are used.

With regard to the second factor above, the very fact that the subscriber (and possibly the relying party as a third party beneficiary) contracts with the CA to issue digital certificates that verify the subscriber's identity suggests that the subscriber is relying upon the CA's skill and judgment to produce suitable certificates.[304] For example, in *Diversified Graphics, Ltd. v. Groves,* in holding that an accounting firm did not exercise the required level of professional care in implementing a "turnkey" in-house data processing system, the court emphasized that it was implicit in the mere *existence of the agreement* that the plaintiff anticipated that the firm possessed superior knowledge in the area and that the plaintiff contracted for the benefit of the firm's expertise (i.e., it was relying on that expertise, especially because a turnkey system implies that the user need do no more than "turn the key" because the experts have already taken care of everything else).[305]

The remaining issue, however, is whether any active selection or furnishing on the part of the seller is occurring. To expand upon an example in the second Official Comment to Section 2-315, if the seller only sells one kind of walking shoe (i.e., one kind of certificate) suitable for ordinary walking around town but it has reason to know that the particular purpose for which that shoe will be used will be heavy-duty mountain climbing (i.e., significant financial transactions) and that the buyer is relying on the seller's skill or judgment in furnishing suitable goods, the seller could end up violating an implied warranty of fitness for a particular purpose if it goes ahead and sells the shoe to the buyer anyway.

Courts could well attribute to a CA the knowledge of the importance of the transactions it facilitates.[306] For example, one could argue that no one would go through the bother of getting a

---

[302] UCC § 2-315, Official Comment 2.

[303] Michael S. Baum, U.S. Dept. of Commerce, Federal *Certification Authority Liability and Policy: Law and Policy of Certificate-Based Public Key and Digital Signatures,* June 1994, at 115.

[304] Michael S. Baum, U.S. Dept. of Commerce, Federal *Certification Authority Liability and Policy: Law and Policy of Certificate-Based Public Key and Digital Signatures,* June 1994, at 115.

[305] *Diversified Graphics, Ltd. v. Groves,* 868 F.2d 293 (8th Cir. 1989).

[306] Michael S. Baum, U.S. Dept. of Commerce, Federal *Certification Authority Liability and Policy: Law and Policy of Certificate-Based Public Key and Digital Signatures,* June 1994, at 115.

certificate if the transaction were not important. It could be argued that if a CA has a range of procedures for issuing certificates, depending on the level of the transaction justifying it, then a selection/furnishing by the CA could be taking place. Conversely, if the CA only has one type of certificate (e.g., the procedure is same for every one, and the CA says it only checks library cards), and if the CA accepts subscriber applications only from banks (where the CA knows that the certificates will in all likelihood be used for significant financial transactions), the CA arguably could be violating the implied warranty of merchantability (as a merchant with respect to goods of that kind). Certificates where the only procedure is checking library cards would not be fit for the ordinary purposes for which such goods are used (i.e., bank use). A court could also examine reliance levels that CAs are permitted to set under digital signature statutes (either by analogy or because the CA is licensed pursuant to that statute) to gauge the importance of the transactions that the certificate is facilitating. If a court charges a CA with this knowledge, it could easily find that the CA is making an implied warranty of fitness for a particular purpose. It thus is not altogether clear exactly what implied warranties arise under the UCC; the ability of the CA to disclaim such warranties will be key to limiting the CA's potential liability.

Under proposed Article 2B, the implied warranty of fitness for a particular purpose has been modified. The first Reporter's Note indicates that, under new Section 405 of Article 2B, if a contract calls for development of information to certain specifications, the licensor's basic obligation is to conform to the agreement and meet the specifications. Likewise, if there are any questions regarding whether the licensee is relying on the licensor's expertise to create a product with characteristics suited to the licensee's intended purpose, the implied warranties Article 2B will impose the additional obligations as provided in the statute.[307] This section is designed to resolve the conflict in development and design contracts regarding whether the appropriate implied obligation is to produce a satisfactory result (goods-oriented) or to make workmanlike efforts (services-oriented). For information contracts where implied warranties are inconsistent with the nature of the contract and fitness of outcome can only be contracted for as an express warranty, such as those commonly associated with the publishing and entertainment industries, the section makes clear that the implied warranty does not arise for published content as to creation or distribution in general.[308]

The CA could disclaim any warranties arising under new Section 405 by stating: "There is no warranty that this information or my efforts will fulfill any of your particular purposes or needs," or use words of similar import.[309] Section 406 also expressly addresses the way to handle disclaimers of implied warranties in mass-market licenses, which arguably are like a CPS (because mass-market licenses are standard form notices that are posted but not signed in the traditional paper sense; acceptance of the terms of a mass-market license in a digital context can occur by clicking an "I accept" button). Under Section 406 of Article 2B, all implied warranties (except for those in Section 2B-401 regarding warranty and obligations concerning quiet enjoyment and noninfringement) can be disclaimed if the language is conspicuous and uses the

[307] National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 405, Reporter's Note 1 (February 1998 draft).

[308] National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 405, Reporter's Note 3 (February 1998 draft).

[309] National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 406(3) (February 1998 draft).

following language or words of similar import: "Except for express warranties stated in this contract, if any, this information is being provided with all faults, and the entire risk as to satisfactory quality, performance, accuracy, and effort is with the user."[310]

5.2.3 Third-Party Beneficiaries of Warranties

Section 2-318 of the UCC extends all warranties arising under the UCC -- whether express or implied -- to certain persons other than the purchaser, on the theory that such persons are third-party beneficiaries of the warranties. This section is drafted with three alternatives, of which most states have adopted one version. The alternative selected will determine whether a person qualifies as a third-party beneficiary:

- **Alternative A** extends the seller's warranties to any natural person in the family or household, including guests in the home of the buyer, if it is reasonable to expect that such person may use, consume, or be affected by the goods and who is *injured in person* by breach of the warranty (the most conservative approach, intended to neither enlarge or restrict the developing case law,[311] which has been adopted by the majority of the states);[312]
- **Alternative B** extends the seller's warranties to any natural person who may be expected to use, consumer, or be affected by the goods and who is *injured in person* by breach of the warranty (for states where the case law has already developed further and for those desiring to expand the class of beneficiaries);[313] and
- **Alternative C** extends the seller's warranties to any person who may reasonably be expected to use, consume, or be affected by the goods and who is injured by the breach of the warranty (the trend of modern decisions as indicated by the Restatement of Torts 2d § 402A in extending the rule beyond injuries to the person).[314]

Two states -- Louisiana and California -- have not enacted UCC Section 2-318 at all.[315] Even among states who have enacted one of the three Alternatives, they have not done so word-for-word. For example, Florida extends the third-party beneficiaries listed in Alternative A to the buyer's employees, servants, or agents.[316] Even states that have adopted the more conservative Alternative A in verbatim form have held that UCC § 2-318 does not prevent extension of the statute's protection to those nonpurchasers not specifically identified in the

---

[310] National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 406(4) (February 1998 draft).

[311] UCC § 2-318, Official Comment 3.

[312] Diane L. Schmauder, *Third-Party Beneficiaries of Warranties Under UCC § 2-318,* 50 A.L.R.5th 327, 348 (1997).

[313] UCC § 2-318, Official Comment 3.

[314] UCC § 2-318, Official Comment 3.

[315] Diane L. Schmauder, *Third-Party Beneficiaries of Warranties Under UCC § 2-318,* 50 A.L.R.5th 327, 348 (1997).

[316] Diane L. Schmauder, *Third-Party Beneficiaries of Warranties Under UCC § 2-318,* 50 A.L.R.5th 327, 348 (1997).

statute.[317] States that have adopted Alternative B sometimes have done so only after tailoring it. For example, Delaware has adopted Alternative B, but omits the "in person" injury requirement.[318] Moreover, states who have enacted either Alternative A or B, whose language requires that the third-party beneficiary be a "natural person," have differed in their holdings as to whether a corporate nonpurchaser could qualify.[319]

Although each of the three Alternatives indicates that "[a] seller may not exclude or limit operation of this section," that does not mean that a seller is precluded from excluding or disclaiming a warranty that might otherwise arise in connection with the sale, so long as that exclusion or modification is permitted by the UCC.[320] It also does not prevent the seller from limiting the remedies of his own buyer (in this case, the subscriber) and of any beneficiaries (in this case, the relying parties) in accordance with applicable provisions of the UCC.[321] On the contrary, "[t]o the extent that the contract of sale contains provisions under which warranties are excluded or modified, or remedies for breach are limited, such provisions are equally operative against beneficiaries of warranties under this section."[322] In other words, the beneficiaries are not blocked by absence of privity from bringing a direct action for breach of warranty against a seller.[323] Yet, the third party's rights are derivative -- they are no greater than those of the buyer.

Proposed Article 2B[324] provides that -- except with regard to *published* information content -- a warranty to a licensee extends to those for whose benefit the licensor intends to supply the information (including, in the case of a consumer, all individuals in the consumer's immediate family or household) and that rightfully use the information in a transaction or application of a kind in which the licensor intends the information to be used. Section 409 also provides that a disclaimer or modification of a warranty, right, or remedies that is effective against the licensee is also effective against any third party under that section.

This approach is consistent with the *Restatement (Second) of Torts,* Section 552, which establishes a limited third-party liability structure for persons who provide information to guide others in business decisions.[325] As the Reporter's Note goes on to indicate, most states currently do not impose liability under a third-party beneficiary theory unless there is a "special

---

[317] Diane L. Schmauder, *Third-Party Beneficiaries of Warranties Under UCC § 2-318,* 50 A.L.R.5th 327, 353 (1997).

[318] Diane L. Schmauder, *Third-Party Beneficiaries of Warranties Under UCC § 2-318,* 50 A.L.R.5th 327, 348 (1997).

[319] Diane L. Schmauder, *Third-Party Beneficiaries of Warranties Under UCC § 2-318,* 50 A.L.R.5th 327, 395-399 (1997).

[320] UCC § 2-318, Official Comment 1.

[321] UCC § 2-318, Official Comment 1.

[322] UCC § 2-318, Official Comment 1.

[323] UCC § 2-318, Official Comment 2.

[324] *See* National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 409 (February 1998 draft).

[325] *See* National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 409, Reporter's Note 5 (February 1998 draft).

relationship" between the information provider and the injured party.[326] As indicated above, the determination of who is a third-party beneficiary is entitled to enforce warranties accorded the buyer will vary from state to state. Nevertheless, disclaimers that exclude intent to affect third parties might help to reduce potential liability under this section.[327]

5.2.4 Ability to Disclaim or Limit Warranties

A CA's ability to disclaim or limit warranties will be restricted by some of the same considerations that affect its ability to limit its own liability (see discussion below). Some special rules arise under the UCC, however, that can affect its ability to disclaim particular types of warranties, as the discussion below indicates.

5.2.4.1 Disclaiming or Limiting Express Warranties

Excluding or limiting any express warranties the CA may be making may be difficult. The UCC requires any such limiting language to be read consistently with the warranty,[328] and thus it is practically impossible to completely negate an express warranty.[329] Because a contract is normally a contract for a sale of something that can be described, a clause that generally disclaims "all warranties, express or implied," cannot reduce the seller's obligation regarding the description and thus can't be given literal effect.[330] A court is unlikely to enforce a disclaimer of express warranty where the CA is not held to any **enforceable performance standards**.[331] This is particularly true when considered against the general UCC requirements of good faith, care, diligence, and reasonableness (i.e., reasonable commercial standards) implied in every contract and that cannot be disclaimed.

For example, subscribers are only willing to purchase a digital certificate (and relying parties are only willing to rely on such a certificate) because the CA's issuance and publication of that certificate mean something -- i.e., that the CA performed some procedure to produce a certificate that provides some indication of the identity of a party and the party's possession of a particular key pair. Because it would be unreasonable to assume that a subscriber who pays for the CA's digital certificates (for the benefit of its relying parties) would agree that the procedures

---

[326] *See* National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 409, Reporter's Note 5 (February 1998 draft).

[327] *See* National Conference of Commissioners on Uniform State Laws, UCC Article 2B § 409, Reporter's Note 8 (February 1998 draft).

[328] UCC § 2-316(1).

[329] UCC § 2-313, Official Comment 4 (except in unusual circumstances, courts won't recognize a material deletion of the seller's obligation). *See also* 1 James J. White and Robert R. Summers, *Uniform Commercial Code,* § 12-2, 12-3, 12-4 (4th ed. 1995) (in some ways, a "disclaimer" of an express warranty seems like an oxymoron).

[330] UCC § 2-313, Official Comment 4.

[331] Michael S. Baum, U.S. Dept. of Commerce, Federal *Certification Authority Liability and Policy: Law and Policy of Certificate-Based Public Key and Digital Signatures,* June 1994, at 112, *citing A&M Produce Co. v. FMC Corp.,* 186 Cal. Rptr. 114, 125 (Cal. Ct. App. 4 Dist. 1982) ("'[s]ince a product's performance forms the fundamental basis for a sales contract, it is patently unreasonable to assume that a buyer would purchase a standardized mass product from an industry seller without any enforceable performance standards.'")

the CA follows in issuing a digital certificate provide no indication as to the identity of that party, a disclaimer of such an express warranty probably would not be effective.

An **integration or merger clause** can also disclaim or limit an express warranty. Such clauses typically provide that the written document is the contract and that prior written or oral communications do not constitute part of the basis of the bargain. Thus, a CA's statements regarding "the general level of authentication or trust associated with using the [CA]" may not create an express warranty, although the [CA] will likely be held to a reasonably high standard."[332] Where the plaintiff claims the express warranty was made outside of the contract itself, the integration clause might function as an effective disclaimer, but such would not be the result in all states.[333]

In evaluating the validity of a disclaimer of an express warranty, courts will also consider whether such a provision is unconscionable (including an analysis of the relative bargaining power of the parties). They may also consider, with regard to integration clauses, a buyer's lack of sophistication with warranties and contracts in general, and with digital certificate agreements in particular. See discussion in this Section 5 regarding unconscionability and bargaining power of the parties.

The best way to limit express warranties is to avoid making them in the first place**.** That means that the CA must be careful in making promises and representations in its various contracts, its CPS, its CRL, its repository, and advertisements.

5.2.4.2 Disclaiming or Limiting Implied Warranties

As discussed above, implied warranties can be completely disclaimed, either by **specific disclaimers** (which are discussed below according to the type of warranty) and by any of the following **general disclaimers**:

- language such as "with all faults" or "as is" that calls the buyer's attention to the exclusion of warranties and makes clear that there are no implied warranties (this would not be much of a selling point for digital certificates, plus it is by no means clear what "with all faults" or "as is" would even mean in the digital certificate context);[334]
- course of dealing, course of performance, or usage of the trade (difficult to do given that the CA is entering a new field where there is no established course of dealing); or

---

[332] Michael S. Baum, U.S. Dept. of Commerce, Federal *Certification Authority Liability and Policy: Law and Policy of Certificate-Based Public Key and Digital Signatures,* June 1994, at 114.

[333] Michael S. Baum, U.S. Dept. of Commerce, Federal *Certification Authority Liability and Policy: Law and Policy of Certificate-Based Public Key and Digital Signatures,* June 1994, at 113, citing instance in California where oral testimony about pre-contract negotiations was admitted even though the parties had an otherwise valid integration clause in their license agreement (involving non-demurrable cause of action for misrepresentation along with breach of warranty action). *Contra, APLications Inc. v. Hewlett-Packard,* 672 F.2d 1076, 1077 (2d Cir. 1982) (integration clause effectively disclaimed brochure) (also cited by Baum).

[334] VeriSign makes such a disclaimer.

- by the subscriber's inspection or refusal to inspect, where a reasonable inspection would reveal the defects.[335]

With regard to **inspection**, several other factors are pertinent.[336] First, to bring the situation within a scenario in which the buyer *refused to examine,* it is not enough that the CA makes the certificate available for inspection. The CA must also demand -- through its contract with the subscriber -- that the subscriber fully examine the certificate, thereby placing the subscriber on notice that it is assuming the risk of defects that an examination would reveal. The CA would also have to demand that relying parties consult the CRL before relying on the published certificate in the repository (and perhaps contractually obligate the subscriber to require the relying parties to consult the CRL for certificates that the CA issues directly to the subscriber). It is not clear, however, whether the CA would be obligated to "push out" CRL information to the relying party or otherwise spell out where to get that information.

Second, the CA should avoid counteracting the effect of its demand for inspection by statements or representations it makes about the certificates' merchantability or specific attributes (essentially, express warranties) if the subscriber clearly indicates that it is relying on those words rather than on the inspection. It is not clear what kinds of statements or representations the CA would be making on the certificate itself, but the CA would certainly need to be careful of any statements or representations it makes in its CPS, CRL, or at its repository.

Moreover, an applicable digital signature statute could arguably be making the CA's representations for it -- i.e., that by issuing a certificate, a licensed CA "certifies to all who reasonably rely on the information contained in the certificate that . . . the information in the certificate . . . is accurate."[337] Unless the applicable digital signature statute imposes an obligation on the subscriber to "inspect," and absent a contractual obligation on the part of the subscriber to inspect, the CA's ability to rely on a duty or refusal to inspect may be extremely limited.

Third, the circumstances under which the buyer must examine the goods can make a difference. Although a subscriber cannot be excused from failing to noticing obvious or patent defects, it can be excused from failing to detect latent defects where the circumstances do not permit the inspection necessary to ascertain such defects. Here again, the issue arises as what the CA's obligations are with regard to the CRL -- i.e., must it push it out to the relying parties, direct such parties to the appropriate location, or otherwise provide an environment conducive to inspection. Again, contractually obligating the subscriber to require relying third parties to review the CPS and consult the CRL before relying on the certificate can be key to reducing the CA's potential liability.

Fourth, the subscriber's skill and sophistication will also come into play in the inspection. A "professional" buyer traditionally will be held to have assumed the risks that a professional in

---

[335] UCC § 2-316(3).

[336] UCC § 2-316, Official Comment 8.

[337] Utah Code Ann. § 46-3-303(3)(a).

the field should have observed, but a nonprofessional buyer will only be held to have assumed the risk for defects that a layman might be expected to observe. It is not clear under which category the relying parties, many of whom could be consumers, would fall, especially given the relative newness of the field. The only "professionals" could well be the CAs themselves. As indicated earlier, the very reason that relying parties would turn to CAs is because they lack the special skills or abilities of a CA.

This lack of ability to inspect in the digital certificate scenario can have significant effects on other provisions of the UCC, such as Section 2-607, which requires that the buyer notify the seller regarding a defect in the good in order to trigger the entitlement to the remedy.[338] Although the relying party lacks the ability to perform an adequate inspection of the certificate (i.e., it cannot determine if the CA's investigation underlying the information was adequate and thus produced a certificate with reliable information), the same cannot be said for the subscriber (the subscriber knows the information because the certificate reflects information about the subscriber). Inability to inspect could be problematic where the defect in the certificate is discovered years later -- i.e., as in the case of a real estate purchase, where the buyer goes to sell the property; the CA could have liability years down the road (long after it goes out of the digital certificate business, for example).

As the discussion above indicates, because general disclaimers can be limited by the circumstances, it is far better in practice to use specific disclaimers to exclude or limit implied warranties.

The **implied warranty of merchantability** can be *specifically* disclaimed in a conspicuous writing that mentions "merchantability." A key issue in determining whether a disclaimer of the warranty is effective is determining whether it is conspicuous. Section 1-201(10) of the UCC provides that a term or clause is conspicuous "when it is so written that a reasonable person against whom it is to operate ought to have noticed it." The section goes on to give examples of conspicuousness:

- a printed heading in capitals (as NON-NEGOTIABLE BILL OF LADING),
- language in the body of a form if it is in larger or other contrasting type or color, or
- any stated term in a telegram.[339]

These are only intended as examples of a few of the methods for calling attention to a contractual term.[340] Only a court can decide whether a term is conspicuous,[341] and the test will be: whether attention can reasonably be expected to be called to it.[342]

---

[338] UCC § 2-607.

[339] UCC § 1-201(10).

[340] UCC § 1-201, Official Comment 10.

[341] UCC § 1-201(10).

[342] UCC § 1-201, Official Comment 10.

The CA's ability to create conspicuous disclaimers and notices will greatly affect its potential liability. It is far from clear, however, what constitutes "conspicuousness" in an electronic or digital certificate context. For Internet transactions, HTML permits the use of colored text and differentiated type faces. Yet, even if a warranty disclaimer is contained in all capital letters, in a different color, and in a different type face, it is unlikely to be enforced if it is buried in the middle of a 98-page CPS that is incorporated by reference in a certificate. This is especially true given the different way that people access documents on the Internet; if the CPS is accessed by the relying party at a Web site, the CA must be able to ensure that the screen displaying the disclaimer and other key terms limiting reliance on, and the meaning of, the certificate will always pop up first.

The **warranty of fitness for a particular purpose** can be *specifically disclaimed* by a conspicuous writing that need not expressly mention fitness for a particular purpose. The warranty can also be *generally disclaimed* by the methods discussed above.

5.2.5 Ability to Contractually Limit Liability

5.2.5.1 UCC Restrictions on Disclaimers and Other Liability Limitations

A guiding principle of the UCC is freedom of contract.[343] Toward that end, the UCC specifies that the *effect* (i.e., the legal consequences)[344] of its provisions may usually be varied by agreement. The *meaning* of the provisions, however, cannot be altered by agreement.[345] For example, parties to a contract cannot agree to change the meaning of terms such as "good faith," "purchase," "conspicuous," or "merchant" as used in the UCC.

The UCC provides two primary exceptions to the parties' ability to agree otherwise. First, when a particular provision of the UCC specifies that its terms cannot be varied by agreement[346] the UCC will apply as enacted. Second, the UCC provides that "the obligations of good faith, diligence, reasonableness and care prescribed by this Act *may not be disclaimed* by agreement. . . ."[347] Nevertheless, the parties may, by agreement, "determine the standards by which the performance of such obligations is to be measured *if such standards are not manifestly unreasonable*."[348]

"Good faith" is a basic principle that runs throughout the UCC, and "every contract *or duty* within this Act imposes an obligation of good faith in its performance or enforcement."[349]

---

[343] UCC § 1-102, Official Comment 2.

[344] UCC § 1-102, Official Comment 2.

[345] UCC § 1-102, Official Comment 2.

[346] UCC § 1-102(3). For example, the requirements of UCC § 2-201 regarding the Statute of Frauds cannot be altered by agreement.

[347] UCC § 1-102(3) (emphasis added).

[348] UCC § 1-102(3) (emphasis added).

[349] UCC § 1-203 (emphasis added).

The general definitions section of Article 1 defines "good faith" as "honesty in fact in the conduct or transaction concerned." The definitions section of Article 2 -- which governs sales -- goes even farther: "'good faith' in the case of a *merchant* means honesty in fact *and the observance of reasonable commercial standards of fair dealing in the trade."*[350] Because a court could conceivably conclude that the CA was a merchant for purposes of the UCC, the CA would be held to the good faith standard applied to a merchant under Article 2. The concept of *reasonable commercial standards* is present in both the definition of "good faith" for merchants and in Section 1-102(3), which permits parties to contractually alter the standards by which performance of obligations is to be measured.[351] Although the UCC does not define "reasonable commercial standards," it does include a section that discusses course of dealing and usage of trade, which arguably could constitute the seller's obligations under the UCC.[352]

Other key UCC restrictions on disclaimers and other limitations of liability include those discussed above in regard to exclusion or modification of warranties, those in UCC Section 2-718 regarding liquidated damages,[353] and those in UCC Section 2-719 regarding contractual modification or limitation of remedy. If warranties are effectively eliminated, the contractual liability limitations will not be so pivotal. Likewise, if a liquidated damages clause or liability cap is effectively included, the fact that a seller breached a warranty will not be as costly for the seller. The CA should consider using both means to limit its potential liability as a CA.

Courts generally will enforce **liquidated damages clauses** but will refuse to enforce penalty clauses. According to the *Restatement (Second) of Contracts,* a predetermined damages provision will be enforced if:

- the amount so fixed is a reasonable forecast of just compensation for the harm that is caused by the breach, and
- the harm that is caused by the breach is incapable or very difficult to accurately estimate.

While Section 2-719(3) of the UCC recognizes the validity of clauses that limit or exclude consequential damages (lost of profits, reputation, business opportunity),[354] that same

---

[350] UCC § 1-103(1)(b) (emphasis added).

[351] UCC § 1-102(3) (emphasis added).

[352] In fact, the Official Comment of UCC § 1-203 indicates that the concept of "good faith" is "further implemented by Section 1-205 on course of dealing and usage of trade." Courts have recognized that usage of trade, custom, or widely shared norms can be the basis of a negligence lawsuit (i.e., a tort claim) against a defendant that deviates from the norms. *See, e.g., In re Eastern Transp. Co. v. Northern Barge Corp.*, 60 F. 737, 740 (2d Cir. 1932) (observing that in most cases, reasonable prudence is common prudence).

[353] UCC § 2-316, regarding exclusion or modification of warranties, specifies in subsection (4) that "[r]emedies for breach of warranty can be limited in accordance with the provisions of this Article on liquidation or limitation of damages and on contractual modification of remedy (Sections 2-718 and 2-719)."

[354] The UCC also imposes a duty of mitigation regarding incidental and consequential damages, i.e., the buyer is only entitled to recovery where it could not reasonably have prevented the loss by cover or otherwise. UCC § 2-715, Official Comment 2.

section makes it clear that they cannot operate in an unconscionable manner.[355] Although limitation of consequential damages for injury to the person in the case of consumer goods is prima facie unconscionable, the section expressly indicates that limitation of damages where the loss is commercial is not unconscionable.[356] Because CA liability for consequential damages could mean virtually limitless exposure[357], the CA must be sure to exclude such damages whenever it can.

Although the UCC specifically allows parties to contractually modify or exclude remedies[358] -- such as through damage caps, liquidated damages clauses, disclaimer of warranties, and exclusions of certain types of damages -- the CA must provide at least some minimum adequate remedies.[359] As the first Official Comment to Section 2-719 indicates, "it is the very essence of a sales contract that at least minimum adequate remedies be available."[360] Moreover, the provisions of an applicable digital signature statute may also affect the CA's ability to contractually modify or exclude remedies.

By rejecting the default terms of the UCC (i.e., warranties, remedies, and so on), and agreeing to different terms in their own written contract, parties can significantly limit their potential liability for contractual breach and some tort liability too. Although contract disclaimers will not necessarily eliminate liability for fraud and similar intentional conduct, they can influence the determination whether reliance was justified under the circumstances and define the intended scope of reliance.[361]

5.2.5.2 Non-UCC Limits on Disclaimers

Courts generally enforce exculpatory clauses unless they violate a state's public policy or something in the social relationship between the parties would dictate against it.[362] Nevertheless, exculpatory clauses are not favored and will be strictly enforced against the benefiting party, especially where that party drafted the clause.[363] Moreover, such clauses must spell out the

---

[355] UCC § 2-719(3) provides that "[c]onsequential damages may be limited or excluded unless the limitation or exclusion is unconscionable." *See also* Official Comment 3.

[356] UCC § 2-719(3).

[357] Michael S. Baum, U.S. Dept. of Commerce, Federal *Certification Authority Liability and Policy: Law and Policy of Certificate-Based Public Key and Digital Signatures,* June 1994, at 120 (this is true even though typically only reasonably foreseeable damages can be recovered under *Hadley v. Baxendale,* 156 Eng. Rep. 145 (1854). *See also* UCC § 2-715, which requires buyers to mitigate damages (unlikely to limit the scope of liability significantly in the case of an imposter, where substantial damage can be inflicted immediately upon the relying party's use of the certificate).

[358] UCC §§ 2-316(4), 2-718, 2-719.

[359] UCC § 2-719, Official Comment 1.

[360] UCC § 2-719, Official Comment 1.

[361] Raymond T. Nimmer, *Information Law,* § 10.14[3], at 10-57.

[362] *Harris v. Walker,* 519 N.E.2d 917, 919 (Ill. Ct. App. 1 Dist. 1987),

[363] *Scott & Fetzer Co. v. Montgomery Ward & Co.,* 493 N.E.2d 1022, 1029 (Ill. 1986); *Harris v. Walker,* 519 N.E.2d 917, 919 (Ill. Ct. App. 1 Dist. 1987); *Restatement (Second) of Contracts,* § 195, Comment b, at 65 (1981).

intentions of the parties with great particularity and will not be construed to defeat a claim not explicitly covered by their terms.[364]

Any exculpatory clause that exempts a party from *tort liability* for harm that was *intentionally or recklessly caused* is generally unenforceable on the grounds of public policy.[365] Conversely, exculpatory clauses exempting parties from tort liability that is *negligently caused* are generally unenforceable on public policy grounds if:

- the term exempts an employer from liability to an employee for injury in the course of employment;
- the term exempts one charged with a duty of public service (i.e., such as a common carrier or public utility or other service) from liability to one to whom that duty is owed; or
- the other party is similarly a member of a class protected against the class to which the first party belongs.[366]

The previous list, however, is not exhaustive. Various jurisdictions may enact their own statutes restricting the power to limit liability for negligence in certain instances.[367] It is also against public policy for sellers of products to be insulated from tort liability for *physical harm* caused by the seller's product unless the term is fairly bargained for and is consistent with the policy underlying that liability.[368] The latter circumstance, however, is unlikely to apply to the CA's activities as a CA.

5.2.5.3 Unconscionability and Relative Bargaining Power as Limits on Disclaimers

Courts generally will not enforce contract provisions that they find to be unconscionable. Under the UCC, for example, if a court finds an entire contract or any of its clauses to have been **unconscionable** at the time it was made, the UCC allows a court to modify the offending provision, enforce the contract without the provision, or even refuse to enforce the entire contract.[369] The UCC also recognizes unconscionability restraints with regard to limitations on damages and remedies, as discussed in this Section 5.

Unfortunately, the concept of unconscionability is not well-defined, and the determination will depend upon the particular facts involved. The principle behind it is the "prevention of oppression and unfair surprise."[370] One factor that could affect such a

---

[364] *Scott & Fetzer Co. v. Montgomery Ward & Co.,* 493 N.E.2d 1022, 1029-1030 (Ill. 1986).

[365] *Restatement (Second) of Contracts,* § 195(1), at 65 (1981).

[366] *Restatement (Second) of Contracts,* § 195(2), at 65 (1981).

[367] *Restatement (Second) of Contracts,* § 195, Comment a, at 66 (1981).

[368] *Restatement (Second) of Contracts,* § 195(3), at 65 (1981).

[369] UCC § 2-302(1).

[370] UCC § 2-302(1), Official Comment 1.

determination is the existence of a fiduciary obligation or confidential relationship (i.e., such as where the CA holds a subscriber's private key).[371] In general, however, the UCC indicates that the basic test of conscionability is:

> whether, in the light of the general commercial background and the commercial needs of the particular trade or case, the clauses involved are so one-sided as to be unconscionable under the circumstances existing at the time of the contract.[372]

Courts have defined an unconscionable bargain as one "'which no man in his senses, not under delusion would make, on the one hand, and which no fair and honest man would accept on the other.'"[373] Unconscionability also encompasses "'an absence of meaningful choice on the part of one of the parties together with contract terms which are unreasonably favorable to the other party.'"[374] The fact that the agreement is a form contract is only one of several factors that a court will consider in determining if an exculpatory or other provision is unconscionable.[375]

Most often, the doctrine has been applied to prevent instances of "commercial sharp practices" by parties with superior bargaining power.[376] **Relative bargaining power** of the parties, however, is just one factor a court considers in determining unfairness or unconscionability.[377] In examining a disparity in bargaining power, the relationship between the parties can be key. Even where a semi-public nature is found to permeate the transaction between the parties, exculpatory clauses will usually be given effect.[378] For example, Illinois will generally enforce such clauses, except in five instances where they could be void as against public policy because of either a special relationship or a disparity in bargaining power: common carrier, innkeeper, bailor-bailee, employer-employee, and landlord-tenant.[379] Specific legislative directives, which can vary from state to state, can also limit the validity and enforceability of provisions that exclude liability for negligence.[380]

---

[371] Dan B. Dobbs, *Law of Remedies,* West Publishing Co. § 10.7 at 708 (1973).

[372] UCC § 2-302, Official Comment 1.

[373] *First Financial Ins. Co. v. Purolator Security, Inc.,* 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979), *citing Hume v. U.S.*, 132 U.S. 406, 410 (1975).

[374] *First Financial Ins. Co. v. Purolator Security, Inc.,* 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979), *citing Williams v. Walker-Thomas Furniture Co.,* 350 F.2d 315, 320 (D.C. 1965).

[375] *First Financial Ins. Co. v. Purolator Security, Inc.,* 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979).

[376] *First Financial Ins. Co. v. Purolator Security, Inc.,* 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979).

[377] *First Financial Ins. Co. v. Purolator Security, Inc.,* 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979).

[378] *Rosenstein v. Standard & Poor's Corp.,* 636 N.E.2d 665, 672 (Ill. Ct. App. 1 Dist. 1993),

[379] *Rosenstein v. Standard & Poor's Corp.,* 636 N.E.2d 665, 672 (Ill. Ct. App. 1 Dist. 1993), *citing Simmons v. Columbus Venetian Stevens Buildings, Inc.,* 155 N.E.2d 372 (Ill. Ct. App. 1 Dist. 1958). *See also First Financial Ins. Co. v. Purolator Security, Inc.,* 388 N.E.2d 17, 20 (Ill. Ct. App. 1 Dist. 1979).

[380] *First Financial Ins. Co. v. Purolator Security, Inc.,* 388 N.E.2d 17, 20-21 (Ill. Ct. App. 1 Dist. 1979) (indicating that state law also prohibited building contractors from limiting their liability via exculpatory provisions in certain instances).

Although the CA's subscriber contracts may be with banks, who typically are regarded as sophisticated entities that are used to entering into contracts in arms-length transactions, many banks will be relatively inexperienced with regard to digital signatures, at least in comparison to the CA. Moreover, because many of the ultimate relying parties are likely to be consumers, the question arises whether the consumer is in a position to fully understand the meaning of the representations and disclaimers made in the CPS or otherwise. For example, because the CA is an expert in the area and followed a certain procedure for verifying identity, the consumer might reasonably infer that the CA procedure is sufficient to ensure the security of the transaction he or she is undertaking. Courts are more likely to enforce exculpatory contracts against sophisticated, experienced parties than they are against inexperienced ones, particularly consumers.[381] As two of the leading commentators on the UCC noted:

> In light of the cases decided thus far, we suspect that whenever a consumer's blood is spilled, even wild horses could not stop a sympathetic court from plowing through the most artfully drafted and conspicuously printed disclaimer clause in order to grant relief. On the other hand, when the buyer is a merchant, no court should apply unconscionability of any variety to a disclaimer that complies with 2-316.[382]

The *Restatement (Second) of Contracts* raises another issue that the CA should keep in mind when evaluating the effect of any opinions or representations it makes. Section 169 of the *Restatement* provides that "[t]o the extent that an assertion is one of opinion only, the recipient is not justified in relying on it," except where the recipient:

- stands in a relation of trust and confidence to the person whose opinion is asserted such that the recipient is reasonable in relying on it (such as a fiduciary relationship);
- reasonably believes that, as compared with himself, the person whose opinion is asserted has special skill, judgment, or objectivity regarding the subject matter (the CA is arguably being engaged precisely because of its special skill and judgment and the inability of relying parties to verify for themselves the information sought in the certificate); or
- is for some special reason particularly susceptible to a misrepresentation of the type involved (i.e., many relying parties and even some subscribers will never have dealt with digital certificates before and may not fully understand the ramifications of their use).[383]

---

[381] *Harris v. Walker,* 519 N.E.2d 917, 920 (Ill. Ct. App. 1 Dist. 1987) (enforced release signed by experienced horse rider who claimed to understand the release he signed; only the most inexperienced of horseback riders would not understand that horse could become spooked under certain circumstances and cause rider to fall); *Gale v. Value Line, Inc.,* 640 F.Supp. 967, 968-969 (D.R.I. 1986) (court noted that plaintiff investor was a lawyer, practicing psychiatrist, and successful investor in convertible securities who decided which information supplied by defendant to ignore and which information to rely on).

[382] 1 James J. White and Robert R. Summers, *Uniform Commercial Code,* § 12-12, at 681 (4th ed. 1995).

[383] *Restatement (Second) of Contracts,* § 169 (1981).

With regard to the first factor, a fiduciary relationship could arise between a CA and a subscriber where the CA holds the private key for a subscriber. It could even arise between a CA and a relying party.[384] The second and third factors may be particularly relevant in a digital certificate context, where many subscribing banks and most relying parties (the bulk of whom might be consumers) do not understand digital signature technology, whereas the CA will be perceived as an expert. It could be argued that even where the CA clearly indicates its procedures (i.e., "we only check library cards"), unsophisticated parties may presume -- because of the CA's position as an expert -- that such procedures are sufficient for all occasions in which the need for a digital certificate might arise. The clarity of the CA's notices will be key in dispelling such notions and limiting the CA's potential liability. The CA's careful control of its advertisements and any other statements it may make about its services and/or goods will also play an important role.

Some courts have indicated that it can be difficult for a plaintiff to argue unconscionability where he clearly had full knowledge of the exculpatory provision and made no attempt to negotiate different terms.[385] The CA should not assume, however, that such circumstances would prevent a court from holding a provision unconscionable. Moreover, there is a serious question as to whether a consumer relying on a certificate ever has full knowledge of the disclaimer.

As the discussion above indicates, the unconscionability issue is not just one of whether the contract was an adhesion contract (i.e., offered on a take-it-or-leave-it basis, where the buyer had no meaningful choice in the matter), or a form contract, or unequal bargaining power, but also one of surprise -- i.e., one which no one in his right senses would accept. Although courts generally enforce standard form or adhesion contracts where there is no ability to bargain regarding the terms, even in consumer contracts,[386] courts sometimes will not enforce a standard clause in a form contract if it constitutes unfair surprise.[387] The risk of a court invalidating a form-contract clause -- such as one limiting warranties or potential damages -- can be reduced by calling the relying party's attention to the provision and obtaining specific, affirmative assent from the relying party to the provision.[388]

For example, the CA should make certain that any key limitations on reliance, warranties, or damages are conspicuously and easily available to the relying party. If such provisions are buried in a 98-page CPS, a court may be more likely to invalidate limits on warranties and liabilities on the theory that it is inherently unreasonable to expect a relying party to wade

---

[384] *See, e.g., Ensminger v. Terminix Int'l Co.,* 102 F.3d 1571, 1574 (10th Cir. 1996) (in case where seller had hired termite inspector for the benefit of buyers, the court indicated that such an unequal relationship where the buyer seeks particular information from a specialist upon which the recipient intends to rely or act may create a fiduciary relationship).

[385] *See, e.g., First Financial Ins. Co. v. Purolator Security, Inc.,* 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979).

[386] Raymond T. Nimmer, *Information Law,* § 11.12[1], at 11-32.

[387] Raymond T. Nimmer, *Information Law,* § 11.12[4][a], at 11-37.

[388] Raymond T. Nimmer, *Information Law,* § 11.12[4][b], at 11-38. Proposed Article 2B expressly takes this approach by stating that a clause that would otherwise be invalid because of surprise will be enforced if the party subject to the clause expressly agreed to the *particular* term.

through 98 pages of text for every certificate it receives from every CA. On the other hand, a one-page synopsis of the major points in conspicuous lettering[389] should increase the likelihood of enforceability.

Given the limited space on a certificate in which to provide disclaimers, and thereby limit third parties' reliance on the accuracy of the information provided in the certificates, the question arises whether notice may be given by incorporation by reference. That is, does simply incorporating provisions of the CPS or other document by reference provide adequate notice to relying parties? This has been a topic of some debate, and the answer is by no means clear. The conspicuousness of the notice referring to the CPS, whether the location where it can be found is specified, and the ease with which it can be accessed are all factors relevant to a court's analysis regarding the enforceability of the disclaimer.

In more traditional settings, a disclaimer's location on a document has been held by courts to be key.[390] Some courts have refused to enforce disclaimers where inconspicuous references were made on the front of a paper-based document to a disclaimer located on the reverse side of the document, while at least two have indicated that the buyer's attention must actually be drawn to a disclaimer on the reverse side.[391] Those courts that have enforced reverse-side disclaimers have done so where the terms were conspicuous (such as larger and heavier print, all capital letters, reference to disclaimer of warranties, and so on).[392] Given that the CA's CPS will not be on the reverse of its certificate, but rather at a completely different location, enforcing the disclaimer will be even more difficult.

5.2.5.4 Limiting Liability Through Exculpatory Clauses

Courts have generally upheld exculpatory clauses where parties have exempted themselves from liability for their own negligence.[393] This general rule not only recognizes parties' freedom to contract, as discussed above, but also that limitations of liability help to keep prices for goods and services affordable.[394]

---

[389] *See* discussion in this Section 5.

[390] 1 James J. White and Robert R. Summers, *Uniform Commercial Code,* § 12-5, at 635 (4th ed. 1995).

[391] 1 James J. White and Robert R. Summers, *Uniform Commercial Code,* § 12-5, at 635-636, including n.16, 17 (4th ed. 1995).

[392] 1 James J. White and Robert R. Summers, *Uniform Commercial Code,* § 12-5, at 635-636, including n.17 (4th ed. 1995), *citing Winter Panel Corp. v. Reichhold Chem., Inc.,* 823 F.Supp. 963 (D. Mass. 1993) ("damages and warranty limitation clause on reverse side were conspicuous because of directive on front to see 'Seller's Standard Terms and Conditions which include a disclaimer of warranties . . . .'").

[393] *See* John T. Coyne, *Effect of Exculpatory Contractual Provisions on Tort Liability to Third Parties,* 31 Tort & Ins. L.J. 785 (Spring 1996). *See also Harris v. Walker,* 519 N.E.2d 917, 920 (Ill. Ct. App. 1 Dist. 1987); *Eaves Brooks Costume v. Y.B.H. Realty*, 556 N.E.2d 1093 (N.Y. 1990).

[394] *See, e.g., Eaves Brooks Costume v. Y.B.H. Realty*, 556 N.E.2d 1093, 1096-97 (N.Y. 1990).

Both commentators and courts alike have noted that the import of an exculpatory clause is its "allocation as to who is to bear the cost of the insurance."[395] If CAs such as the CA were burdened with the obligation to act as insurers of transactions (which unlimited liability without enforceable exculpatory clauses might entail), they would be forced to purchase staggering amounts of insurance (and pass that cost onto their subscribers), be driven to insolvency should even one major transaction go awry because of a faulty certificate, or not even enter the fledgling digital certificate arena in the first place.

In the analogous case of alarm system providers[396] courts have repeatedly recognized that exculpatory clauses function as a means of apportioning the burden of obtaining insurance coverage. It would make no sense to force the alarm contractor to function as an insurer against a risk, "the amount of which they might not know and cannot control," thereby resulting in higher insurance premiums passed on to all those acquiring alarm services (in effect, those with the least to lose would end up subsidizing the cost of protection for those whose potential loss is the greatest).[397] As one court noted, "[p]resumptively insurance companies who issue such policies base their premiums on their assessment of the value of the property and the vulnerability of the premises. No reasonable person could expect that the provider of an alarm service would, *for a fee unrelated to the value of the property,* undertake to provide an identical type coverage should the alarm fail to prevent a crime."[398] To analogize, CAs who issue digital certificates do not base their fees on the value of the property (although some digital signatures statutes do at least contemplate the ability of CAs to set reliance limits) or the vulnerability of the subscriber or relying party; it also seems unreasonable to expect CAs to be liable for all consequential damages flowing from a negligently issued certificate for a minimal, flat fee unrelated to the value of the property. Moreover, courts have recognized that, at the time the contract is executed, there is no reasonable basis on which to predict the nature and extent of any loss or how much of the loss the alarm company's failure of performance might account for, thereby making it extremely difficult to fix actual damages.[399] The same would hold true for CAs.

Courts in these cases have also recognized other key considerations. First, that operators of business establishments should, and often do, carry insurance for loss due to various sorts of crime. Second, that the real cause of the loss was the criminal propensities of the perpetrator, not the failure of the alarm system (i.e., one can't sustain a claim against an alarm company that amounts to a duty to prevent crime).[400] Third, the alarm company is not an insurer against

---

[395] *See* John T. Coyne, *Effect of Exculpatory Contractual Provisions on Tort Liability to Third Parties,* 31 Tort & Ins. L.J. 785 (Spring 1996).

[396] In acting as a CA, the CA may be functioning somewhat as a provider of security: it is providing information that helps to increase the relying party's security that it will not be harmed by a bad actor (an imposter impersonating the subscriber); if the certificate sounds an alarm when a bad actor comes along, substantial loss to the buyer or third parties could be averted.

[397] *Eaves Brooks Costume v. Y.B.H. Realty*, 556 N.E.2d 1093 (N.Y. 1990).

[398] *Guthrie v. American Protection Industries,* 160 Cal. App. 3d 951, 954 (Cal. Ct. App. 2 Dist. 1984).

[399] *Guthrie v. American Protection Industries,* 160 Cal. App. 3d 951, 954 (Cal. Ct. App. 2 Dist. 1984).

[400] *Guthrie v. American Protection Industries,* 160 Cal. App. 3d 951, 954 (Cal. Ct. App. 2 Dist. 1984). *But see Helm v. K.O.G. Alarm Co.,* 4 Cal. App. 4th 194 (Cal. Ct. App. 4 Dist. 1992). There, the court recognized that although

burglary because such systems can be disabled[401] (just as a CA cannot be an insurer against certificates that fail to identify imposters because procedures for issuing such certificates are not foolproof).

As a result, most jurisdictions have upheld provisions limiting liability and damage amounts under burglar alarm service agreements, holding that they are neither unconscionable nor against public policy.[402] The disclaimers used in these alarm system contracts share certain characteristics. They typically provide that:

- the alarm company is **not an insurer** (almost always the first clause of the disclaimer);
- the **subscriber should carry its own insurance** to cover any losses;
- **payments** made under the contract are **based solely on the value of the service** in the maintenance of the system described;
- the alarm company makes **no guarantee or warranty**, including any implied warranty of merchantability or fitness for a particular purpose, or that the system or services supplied will avert or prevent occurrences or the consequences that the system or services were designed to detect, or that the system may not be circumvented or compromised;
- the subscriber does not desire the contract to provide for full liability of the alarm company and that the alarm company shall be **exempt from liability** from loss or damage directly or indirectly stemming from occurrences or consequences **that the system was designed to detect or avert**;
- that, given the nature of the service to be rendered, it is **extremely difficult to fix the actual damages**, if any, that may proximately result from a failure of the system to work properly or from the alarm company's failure to perform the services or any of its obligations under the contract;
- **damage caps** (liability of no more than a specified dollar amount) or **liquidated damages** (set dollar amount) (often a percentage of the annual service charge) as the exclusive remedy;
- that the **damage limits apply irrespective of cause or origin** resulting in direct or indirect damage to person or property, whether from performance or nonperformance of the obligations imposed by the contract or by the negligence (active or otherwise) of the alarm company, its agents, or its employees;

---

alarm systems can't be said to absolutely prevent crime, it is quite another thing to say that properly working alarm systems can't lessen the loss occasioned by criminal acts. Nonetheless, the plaintiffs in this case lost because they never proved the factual causal nexus between their reliance on the intentional misrepresentations -- that the alarm would work with phone lines cut -- and the unmitigated theft/arson losses they suffered (i.e., other factors, such as fire and police unit response times, also played a role). Alarm systems, like CA-issued certificates, are also designed to act as a deterrent in the first place and to assist in the detection (and apprehension) of the undeterred intruder. *Guthrie v. American Protection Industries,* 160 Cal. App. 3d 951, 954 (Cal. Ct. App. 4 Dist. 1984).

[401] *Fretwell v. Protection Alarm Co.,* 764 P.2d 149, 152 (Okla. 1988).

[402] *Fretwell v. Protection Alarm Co.,* 764 P.2d 14, 151 (Okla. 1988), *citing cases cited in Morgan,* 246 N.W.2d at 447; *Central Alarm of Tucson v. Ganem,* 116 Ariz. 74, 567 P.2d 1203, 1206-1207 (Ariz. Ct. App. Div. 2 1977).

- that if the subscriber desires the alarm company to assume **greater liability** or responsibility to either the subscriber or its insurance carrier by way of subrogation, an **additional price must be quoted** (or that the subscriber releases and discharges the alarm company from all hazards covered by the subscriber's insurance and that no insurance company or insurer will have any right of subrogation against the alarm company);
- that **if any person not a party to the agreement** (including the subscriber's insurance company) **makes any claim** or files any lawsuit against the alarm company for any reason whatsoever (including but not limited to installation, maintenance, operation, or nonoperation of the alarm system), that the subscriber agrees to **indemnify, defend, and hold the alarm company harmless** from any and all claims and lawsuits, including the payment of all damages, expenses, costs, and attorneys fees, whether they are based on active or passive negligence (misfeasance or nonfeasance) on the part of the alarm company, its agents, servants, or employees.

Thus, many alarm companies -- even where they have admitted to breach of contract and negligence in failing to keep the system operable -- have successfully limited their liability to a damage cap/liquidated damages amount.[403]

Courts have also examined the *nature of the contract* entered by the parties -- i.e., how the parties described the basis of the bargain. For example, in *First Financial Insurance Co. v. Purolator Security, Inc.,* the court found that:

> Defendant agreed to provide central station intrusion and hold-up alarm service, not to physically secure the currency exchange premises. As the contract repeatedly emphasizes, defendant did not undertake to insure the currency exchange in case of burglary nor underwrite any risk of loss. The compensation received by defendant related to the value of the services it agreed to perform and is unrelated to the value of the property on the premises. Moreover, the currency exchange independently obtained insurance from plaintiff to cover burglary losses. From the totality of the circumstances, this appears to be an arms-length transaction based on reasonable commercial considerations which are neither one-sided nor unconscionable.[404]

One exculpatory provision in the list above deserves particular attention: indemnification. The prevailing rule is that "a contract may validly provide for the indemnification of one against, or relieve him from liability from, his own future acts of negligence provided the indemnity against such negligence is made unequivocally clear in the contract."[405] Such indemnification clauses tend to be strictly construed, but generally they are

---

[403] *See, e.g., Guthrie v. American Protection Industries,* 160 Cal. App. 3d 951, 953 (Cal. Ct. App. 2 Dist. 1984).

[404] *First Financial Ins. Co. v. Purolator Security, Inc.,* 388 N.E.2d 17, 22 (Ill. Ct. App. 1 Dist. 1979) (also finding no special legal relationship or overriding public interest that would render contract exclusions ineffectual).

[405] *Fretwell v. Protection Alarm Co.,* 764 P.2d 149, 152 (Okla. 1988), *citing* 41 *Am. Jur. 2d* § 9 (1968).

enforceable.[406] The inclusion of such indemnification provisions is key to limiting liability against third-party beneficiaries attempting to claim benefits under the contract.

For example, in *Scott & Fetzer Co. v. Montgomery Ward & Co.,*[407] although the alarm company had many of the standard exculpatory clauses outlined above (including the one providing that damage limits apply irrespective of cause or origin resulting in direct or indirect damage to person or property), those provisions did not affect the alarm company's duties to the adjacent tenants. The court emphasized that indemnification clauses must be strictly construed, and must clearly exempt the alarm company from its own negligence, and that the exculpatory clause in this contract may be construed to apply to actions in contract or tort but only to the subscriber and possibly to the property of others located on the subscriber's property. The court distinguished the case from another with similar facts that reached a seemingly different result; the difference, the court stressed, was because the contract in the other case also contained an indemnification clause.[408] The court also indicated that the parties' contract lacked any language explicitly covering third-party actions for contribution.[409]

Parties may also limit their liability through releases, otherwise known as exculpatory contracts, which are defined as agreements to "release one or more individuals or entities from liability resulting from any negligent act or omission or other wrongful conduct committed by those individuals or entities."[410] Such releases are signed as a condition precedent to some activity (often dangerous in nature), such as driving on a racetrack or renting a horse to go horseback riding. To determine whether such an exculpatory contract is enforceable, courts will first determine whether the clause is void and unenforceable on public policy grounds (including exclusions of liability for intentional or reckless acts, exclusions for physical harm in cases of product liability, etc.).[411] As part of this analysis, a court may consider whether such agreements are generally enforceable in the particular context (e.g., in the car racing context, most jurisdictions recognize and enforce exculpatory clauses).[412] They will also consider whether there is something in the social relationship of the parties that militates against upholding such an agreement (e.g., employer-employee, tenant-landlord, and the like, as discussed in this Section 5.[413] Second, courts will examine whether the terms of the contract clearly express the intent of

---

[406] *Fretwell v. Protection Alarm Co.,* 764 P.2d 149, 152 (Okla. 1988).

[407] *Scott & Fetzer Co. v. Montgomery Ward & Co.,* 493 N.E.2d 1022 (Ill. 1986).

[408] "In the event any person, not a party to this agreement shall make any claim or file any lawsuit against the contractor for failure of its equipment or service in any respect, subscriber agrees to indemnify, defend and hold harmless from any an all such claims and lawsuits including the payment of all damages, expenses, costs, and attorney's fees." *Scott & Fetzer Co. v. Montgomery Ward & Co.,* 493 N.E.2d 1022, 1028 (Ill. 1986), *citing Allendale Mut. Ins. Co. v. Leaseway Warehouse, Inc.,* 624 F. Supp. 637, 638 (N.D. Ill. 1985).

[409] *Scott & Fetzer Co. v. Montgomery Ward & Co.,* 493 N.E.2d 1022, 1030 (Ill. 1986).

[410] *Cadek v. Great Lakes Dragaway, Inc.,* 843 F.Supp. 420, 421-422 (N.D. Ill. 1994) (such agreements, although they can effectively exclude negligence, do not always excuse liability for breach of contract or misrepresentation).

[411] *Cadek v. Great Lakes Dragaway, Inc.,* 843 F.Supp. 420, 421-422 (N.D. Ill. 1994) (applying Wisconsin law); *Harris v. Walker,* 519 N.E.2d 917, 919 (Ill. Ct. App. 1 Dist. 1988).

[412] *Cadek v. Great Lakes Dragaway, Inc.,* 843 F.Supp. 420, 422 (N.D. Ill. 1994).

[413] *Harris v. Walker,* 519 N.E.2d 917, 919 (Ill. Ct. App. 1 Dist. 1988).

the parties, in light of the surrounding circumstances, so that it is evident that the parties knowingly agreed to excuse one of them from acts for which that party would otherwise be responsible.[414]

Courts have upheld such exclusionary contracts despite the fact that they are often take-it-or-leave-it sorts of contracts. The mere fact that one would not be allowed to use the racetrack, for example, if he had not signed the release does not rise to the level of economic or other compulsion.[415] Moreover, the plaintiffs in such cases voluntarily chose to enter into a relationship with the defendant whereby the plaintiff agreed to assume the risks associated with the activity, with full knowledge and appreciation of the danger.[416] Likewise, if the CA could secure some acceptance of a similar release in the digital certificate context (e.g., clicking on an "I accept" icon contained in the CPS), assuming that the release adequately disclosed the danger, defined the CA's undertaking, and made clear that the relying party was assuming the risk of the activity, an exculpatory contract could be an effective means of limiting the CA's liability to relying third parties, in addition to contractual limitations placed in the CA's agreements with subscribers.

Exculpatory clauses have been particularly effective in limiting liability in information-provider contracts as well, as discussed in this Section 5. The effect of such clauses on third-party beneficiaries is discussed in the next section.

5.2.5.5 Third Party Beneficiaries

Many of the cases involving information providers involve plaintiffs claiming third-party beneficiary status -- i.e., they were not one of the parties signing the contract. Typically, contracts between two parties only confer benefits on those two parties. When parties contract for the benefit of a third party, as the CA and the subscriber arguably would be doing, the question arises as to what rights those beneficiaries would have if the agreement is breached. Only *intended* beneficiaries may sue in the event of a contractual breach. Merely receiving benefits from the contract is not enough to confer intended beneficiary status. Parties not meeting the definition of an intended beneficiary -- one for whose benefit the contract is made -- are *incidental* beneficiaries and are thus not entitled to sue for contractual breach.

To hold that a third party was intended to be a beneficiary, the court must first find that this would accomplish the intentions of the parties and that either the performance of the contract was intended to satisfy an obligation owed by the promisee to the beneficiary, or that circumstances indicate that the promisee intended to give the beneficiary the benefit of the promised performance. Courts determine such intent by examining the following factors:

- Was the beneficiary named in the contract?
- Was performance supposed to be made directly to the promisee?

---

[414] *Cadek v. Great Lakes Dragaway, Inc.,* 843 F.Supp. 420, 422 (N.D. Ill. 1994).

[415] *Harris v. Walker,* 519 N.E.2d 917, 920 (Ill. Ct. App. 1 Dist. 1988).

[416] *Harris v. Walker,* 519 N.E.2d 917, 920 (Ill. Ct. App. 1 Dist. 1988).

- Could the beneficiary alter the performance terms?
- Could the beneficiary have reasonably relied on the contract?

The language of the contract can be key in determining the intent of the parties regarding the existence of a third-party beneficiary relationship. For example, in *Lockwood v. Standard & Poor's Corp.,*[417] a court cited exclusivity[418] and integration[419] clauses as evidencing an intent not to confer a third-party benefit. Because the license agreement appeared to be wholly integrated, the court refused to examine extrinsic evidence of the plaintiff's status.[420] The court emphasized that mere mention in the license agreement of the plaintiff's "agent" (the Options Clearing Corporation, which settles S&P index options) as a "special recipient of closing index values" did not confer third-party beneficiary status on the plaintiff.[421] Moreover, even assuming that OCC acted as a settlement agent for the plaintiff and other options investors, retaining such a third party to assist in the performance by the promisee did not mean that the plaintiff was an intended beneficiary of the main contract.[422]

Many courts hold that even if a relying party qualified as an intended third-party beneficiary of an agreement, that relying party's rights would be *derivative* and subject to the same defenses available to the contracting party. Thus, even if the contract includes a warranty from the information provider that it will promptly correct errors brought to its attention, if the agreement also expressly disclaims any guarantee of accuracy and/or the completeness of the information, the relying party's recovery will be limited. Such third-party beneficiaries would be subject to any contractual limits on damages agreed to by the contracting parties.[423]

---

[417] *Lockwood v. Standard & Poor's Corp.*, 682 N.E.2d 1227 (Ill. Ct. App. 1 Dist. 1997). This case involving S&P is based on remarkably similar facts to *Rosenstein*, where another investor sued for breach of contract under a third-party beneficiary theory and for negligent representation. Unlike the *Rosenstein* court, however, the *Lockwood* court found that S&P owed no duty to the plaintiff. The plaintiff claimed that options investors such as the plaintiff, through their settlement agent OCC, were third-party beneficiaries. Applying New York law in interpreting the license agreement (though Illinois law governed the suit generally), the court emphasized that "an intended third-party beneficiary may enforce a contract if he is the only party who can recover if the promisor breaches the contract or if the contract language indicates an intention to permit enforcement by the third party." The court found nothing in the express language of the license agreement that indicated an intention to benefit a third-party beneficiary.

[418] "Agreement is solely and exclusively between the parties as presently constituted and shall not be assigned or transferred." *Lockwood v. Standard & Poor's Corp.,* 682 N.E.2d 1227 (Ill. Ct. App. 1 Dist. 1997).

[419] "Agreement constitutes the entire agreement of the parties hereto with respect to its subject matter and may be amended or modified only by a writing signed by duly authorized officers of both parties. ... There are no oral or written collateral representations, agreements, or understandings except as provided herein." *Lockwood v. Standard & Poor's Corp.,* 682 N.E.2d 1227 (Ill. Ct. App. 1 Dist. 1997).

[420] *Lockwood v. Standard & Poor's Corp.,* 682 N.E.2d 1227 (Ill. Ct. App. 1 Dist. 1997), *citing Hylte Bruks Aktiebolag v. Babcock & Wilcox Co.,* 399 F.2d 289, 293 (2d Cir. 1968).

[421] *Lockwood v. Standard & Poor's Corp.,* 682 N.E.2d 1227 (Ill. Ct. App. 1 Dist. 1997).

[422] *Lockwood v. Standard & Poor's Corp.,* 682 N.E.2d 1227 (Ill. Ct. App. 1 Dist. 1997).

[423] *Lockwood v. Standard & Poor's Corp.,* 682 N.E.2d 1227 (Ill. Ct. App. 1 Dist. 1997).

Courts are divided as to whether third party *tort* claims are subject to exculpatory contractual provisions that limit the promisor's liability to the promisee.[424] Exculpatory clauses do not affect liability where there is a duty to refrain from affirmatively injurious conduct (cause of action arises independent of contract); disclaimers in such cases are only effective against those agreeing to the disclaimer. One key question is whether the undertaking to provide services is the basis for the tort claim or if it is merely incidental. Absent an undertaking -- as in contract -- there is no legal obligation to confer a benefit.

One key issue is whether the CA can be said to be forming a contractual relationship with relying parties, who are arguably the intended beneficiaries of the CA's agreement with its subscribers. Although many of these relying parties may have claims arising in tort, the use of contractual disclaimers and other notices may help to limit some of the CA's exposure. Because a major source of potential liability for the CA will stem from losses sustained by relying parties, the issue of whether a contract has, in fact, been formed with such parties will be critical to the CA's ability to limit such liability.

The effectiveness of a disclaimer or any statement limiting reliance on the information to designated parties depends in some measure on the specificity of the terms and their resulting effect on actual or reasonable reliance in defining the scope of the information provider's undertaking. For example, in *Paracor Fin. v. General Elec.,* investors could not demonstrate reasonable reliance on the financial information provider's representations in the case of a leveraged buyout where they had signed an agreement that indicated their decision to purchase was made "without relying on any other person." Part of the court's decision, however, rested on the notion that the investor plaintiffs also were provided access to the information, which would not be the case where a relying party is relying on the CA's information contained in the certificate. Nevertheless, the analogy might hold where the relying party was given access to the CRL and failed to take full advantage of it.

A conspicuous disclaimer regarding the accuracy or inaccuracy of the information provided may help to preclude negligent misrepresentation claims.[425]

Most tort claims that a relying party is likely to bring would arise out of the contractual relationship between the CA and the subscriber. Absent that agreement, the CA would be under no affirmative duty to confer a benefit to anyone. Torts arising out of a contractual relationship closely resemble an action for pure breach of contract and exhibit characteristics of both tort and contract actions.[426] A breach of contract occurs when a party fails to perform a duty arising under or imposed by agreement, while a tort is a violation of a duty imposed by law independent

---

[424] *See* John T. Coyne, *Effect of Exculpatory Contractual Provisions on Tort Liability to Third Parties,* 31 Tort & Ins. L.J. 785 (Spring 1996).

[425] *See, e.g., Gale v. Value Line, Inc.* 640 F. Supp. 967 (D.R.I. 1986), where disclaimer failed because it disclaimed only for the errors of others ("Factual material is obtained from sources believed to be reliable but cannot be guaranteed.") and not also the financial information provider's own mistakes (a statement that "The publisher is not responsible for any error or omissions" would have excused its own negligence.). Although the disclaimer failed, the court found that no express or implied warranties arose, because the publisher never assumed the responsibility of 100% accuracy.

[426] *Fretwell v. Protection Alarm Co.,* 764 P.2d 149, 151 (Okla. 1988).

of contract.[427] Many courts have held that in cases where the contract established the duty, any lawful limitations in the contract may also limit the liability of the defendant.[428] Even where there are third-party beneficiaries to the contract, a contract establishing a duty to third-party beneficiaries can limit the liability of the promisor because the consideration for the contract was set by the parties with such limitations in mind.[429]

5.2.6 Effect of State Digital Signature Acts on Warranties and Limitations of Liability

Analysis of the CA's ability to exclude or limit implied warranties cannot stop with an examination of the UCC provisions. The CA's ability to disclaim warranties and otherwise limit its liability contractually may be limited by the default provisions of any **applicable state digital signature legislation**.[430] In this analysis, we focus on the Utah Digital Signature Act because it was the first comprehensive digital signature legislation to be enacted, and has served as a model for other states that have either passed or are considering such legislation.

Under the Utah Act, a licensed CA[431] is deemed to make certain warranties to *subscribers* upon issuing a certificate:

- that the certificate contains no information known to the CA to be false,
- that the certificate satisfies all material requirements of the Utah Act,
- and that the CA has not exceeded any limits of its license in issuing the certificate.[432]

The Utah Act prohibits a licensed CA from disclaiming or limiting these warranties.[433] Furthermore, a licensed CA is deemed to represent to the subscriber -- *unless the CA and the subscriber agree otherwise* -- that it will act promptly to suspend or revoke a certificate according to the statutory requirements and that it will notify the subscriber within a reasonable time of any facts known to the CA that significantly affect the validity or reliability of the certificate.[434]

By issuing a certificate, a licensed CA is also deemed under the Utah Act to make certain representations (i.e., the CA "certifies") to *relying parties* (i.e., all who reasonably rely on the information in the certificate):

---

[427] *Fretwell v. Protection Alarm Co.,* 764 P.2d 149, 151 (Okla. 1988).

[428] *See, e.g., Fretwell v. Protection Alarm Co.,* 764 P.2d 149, 151 (Okla. 1988).

[429] *Fretwell v. Protection Alarm Co.,* 764 P.2d 149, 151 (Okla. 1988).

[430] Indeed, UCC § 1-103 indicates that all supplemental bodies of law continue to apply to commercial contracts except to the extent that they are explicitly displaced by the UCC. *See also* UCC § 1-103, Official Comment 1.

[431] Under the Utah Act, license is voluntary.

[432] Utah Code Ann. § 46-3-303(1)(a).

[433] Utah Code Ann. § 46-3-303(1)(b).

[434] Utah Code Ann. § 46-3-303(2).

- that the information in the certificate and listed as confirmed by the CA is accurate;
- that all foreseeable information material to the reliability of the certificate is stated or incorporated by reference within the certificate;
- that the subscriber has accepted the certificate; and
- that the licensed certification authority has complied with all applicable Utah state laws governing issuance of the certificate.[435]

The weight of these representations and warranties to subscribers and relying parties, which are triggered by the CA's issuance of a certificate, is increased by Section 46-3-302's conditions under which a licensed CA may issue a certificate. The licensed CA may only issue a certificate to a subscriber after *all* of the following conditions have been satisfied:

- the CA has received a request for issuance signed by the prospective subscriber; and
- the CA has confirmed that:
  - ✓ the prospective subscriber is the person to be listed in the certificate to be issued,
  - ✓ if that subscriber is acting through an agent, the subscriber has authorized the agent to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key,
  - ✓ the information in the certificate to be issued is accurate after due diligence,
  - ✓ the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate,
  - ✓ the prospective subscriber holds a private key that can create a digital signature, and
  - ✓ the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber.[436]

These requirements cannot be waived or disclaimed by either the licensed CA or the subscriber.[437] Thus, in the event that the substantive law of the Utah Act, or a similar state statute, applies to the CA's activities, the CA must -- in assessing the scope of its potential liability -- recognize that a licensed CA will be deemed to be making the above warranties and representations. Although the existence of the warranties and representations will not be in doubt (because the statute establishes their existence), their exact scope may not always be clear. The commentary section and any legislative history will play a key role in interpreting the scope of these warranties and representations. At least in the beginning, because the statute is so new, there will be little or no case law for the CA to rely on, except for cases that apply by analogy only (i.e., notary public and accountant liability cases).

Thus, assuming that the warranty liability is triggered (i.e., the warranty exists, the CA has breached the warranty, and that the breach caused the loss),[438] the next question is: what is the scope of the CA's liability for such breach of warranty? Although the Utah Act imposes

---

[435] Utah Code Ann. § 46-3-303(3).

[436] Utah Code Ann. § 46-3-302(1)(a), (b).

[437] Utah Code Ann. § 46-3-302(1)(c).

[438] See discussion of the common law action for misrepresentation.

potential warranty liability on licensed CAs, it also limits the scope of the potential liability (unless the CA waives its application) with regard to relying parties. First and foremost, the Utah Act provides that the CA is liable only for "direct, compensatory damages" in any action to recover losses due to reliance on the certificate; the Utah Act specifically excludes punitive or exemplary damages; pain and suffering damages; and damages for lost profits, savings, or opportunity (consequential damages).[439] Because consequential damages represent perhaps the greatest damage risk that the CA faces, the applicability of this provision could be key.

Second, the statute specifies that the CA will not be liable for "any loss caused by reliance on a false or forged digital signature of a subscriber," if the CA complied with all of the material requirements of the Utah Act.[440] Again, definition of and adherence to the necessary procedures, and establishment of proper recordkeeping practices to demonstrate that fact, will be key in limiting the potential scope of the CA's liability.

Third, the CA will not be liable in excess of the amount specified in the certificate as its recommended reliance limit for either:

- losses caused by reliance on a misrepresentation in the certificate of any fact that the licensed authority is required to confirm, or
- failure to comply with the statutory requirements of Section 46-3-302 in issuing the certificate.[441]

With regard to the latter provision, it is not clear how much protection from liability it affords. Although it indicates that the issuance provisions enumerated above will only trigger liability up to the reliance limit, the issuance provisions do not stand alone, but rather are incorporated as part of the warranties above. For example, regarding warranties made to subscribers, the CA warrants that the certificate satisfies all material requirements of the Utah Act and that the CA has not exceeded any limits of its license in issuing the certificate;[442] all material requirements of the Utah Act certainly include, and limits of the license could arguably include, the statutory requirements in Section 46-3-302. Regarding warranties made to relying parties, the CA certifies that it has complied with all applicable Utah state laws governing issuance of the certificate;[443] all applicable Utah laws governing issuance of the certificate certainly includes the statutory requirements in Section 46-3-302.

Moreover, another provision of the Utah Act specifies that the liability limits of Section 46-3-309 do not apply to unlicensed certification authorities.[444] A licensed certification authority acts as unlicensed certification authority under the Utah Act "when issuing a certificate

---

[439] Utah Code Ann. § 46-3-309(2)(c).

[440] Utah Code Ann. § 46-3-309(2)(a).

[441] Utah Code Ann. § 46-3-309(2)(b).

[442] Utah Code Ann. § 46-3-303(1)(a).

[443] Utah Code Ann. § 46-3-303(3).

[444] Utah Code Ann. § 46-3-201(6).

exceeding the limits of the license."[445] Although the previous line discusses some of the potential limits of the scope of a license (i.e., maximum number of outstanding certificates, cumulative maximum of recommended reliance limits in certificates issued by the CA, or issuance only within a single firm or organization), it is not clear that those are the only limits of the license. For example, it is not clear from the statutory language whether the following statutory requirements constitute a limit of the license:

- not conducting one's business in a manner that creates an unreasonable risk of loss to subscribers, relying parties, or a repository;[446]
- that a licensed CA or subscriber shall use only a trustworthy system, or that a licensed CA shall disclose any material certification practice statement and any fact material to either the reliability of a certificate that it has issued or to its ability to perform its services;[447]
- the certificate revocation requirements;[448] or
- the requirements to obtain and retain a license (such as not employing felons or those convicted of fraud/deceit crimes, employing personnel who have demonstrated knowledge and proficiency, having the right to use a trustworthy system, and so on).[449]

The Commentary to the Utah Act specifies that an unlicensed CA can issue reliable and legally valid digital certificates, but it also indicates that those who choose to operate without a license undertake greater risk of liability.[450] Thus, determining what constitutes "exceeding the limits of the license" will be key to assessing the potential protection afforded by the Utah Act with regard to damages, particularly consequential damages.

Although the Utah Act provision that prohibits a CA from conducting its business "in a manner that creates an unreasonable risk of loss" to subscribers, relying parties, or repositories seems like language that increases the CA's potential obligations, and thus liabilities, the opposite may, in fact, also be true. That is, it implicitly suggests that subscribers, relying parties, and repositories are not entitled to assume no risk of loss (i.e., that the CA assumes all risk of loss); instead the provision acknowledges that a CA may conduct its business in such a way that there is some reasonable risk of loss to subscribers, relying parties, and repositories. A court might rely on such a provision in applying a rule of reason to the amount of damages that can be imposed on a CA if it has adhered to reasonable procedures.

A further limit on potential CA liability arising from representations and warranties imposed on CAs by the Utah Act can be found in Section 46-3-502 regarding the liability of

---

[445] Utah Code Ann. § 46-3-201(3)(b).

[446] Utah Code Ann. § 46-3-204(1). This provision does indicate, however, that it applies to all CAs, "whether licensed or not."

[447] Utah Code Ann. § 46-3-301.

[448] Utah Code Ann. § 46-3-307.

[449] Utah Code Ann. § 46-3-201(1).

[450] Commentary to the Utah Digital Signature Act, at 9 (Web site page).

repositories. The statute expressly indicates that a repository will be liable for loss incurred by a relying party who reasonably relied on a digital signature verified by the public key listed in a suspended or revoked certificate if: (1) the loss was incurred more than one business day after the repository received a request to publish notice of the suspension or revocation, and (2) the repository had failed to publish the notice of suspension or revocation when the person relied on the digital signature.[451] Liability in such an instance cannot be disclaimed by the repository or otherwise contractually modified (even if the repository, CA, and subscriber all agree).[452] The extent of the repository's damages liability, however, will be limited to the amount specified in the certificate as the recommended reliance limit.[453]

The section also places other limits on the repository's liability. The repository will *not* be liable in a number of instances:

- for failing to publish notice of a suspension or revocation, unless the repository has received notice of publication and one business day has elapsed since the notice was received;
- for misrepresentation in a certificate published by a licensed CA;
- for accurately recording or reporting information that a licensed certification authority or particular Utah officials or bodies have published as provided in the Utah Act, including information about suspension or revocation of a certificate; and
- for reporting information about a CA, certificate, or a subscriber if published according to the statutory requirements or by order of particular Utah bodies;
- for punitive or exemplary damages, pain and suffering damages, and damages for lost profits, savings, or opportunity.[454]

These repository liability provisions will necessarily affect CA liability because they expressly carve out instances in which repository liability will or will not be imposed.

The CA's potential liability can also be limited by Section 46-3-304, which outlines the liability of a subscriber in accepting a certificate. Upon accepting a certificate, subscribers undertake to indemnify the issuing CA for loss or damage caused by an intentional or negligent material misrepresentation or failure to disclose.[455] This indemnification may not be contractually disclaimed or limited in scope.[456] Of course, such indemnification is only as good as the subscriber or subscriber agent's financial ability to come through in the event of loss. Because the CA plans to deal exclusively with banks, these indemnification provisions could at least reduce some of the CA's out-of-pocket losses. Yet, subscriber indemnification can cut two ways: if a CA uses another CA to cross-certify certificates it issues, the CA itself undertakes to indemnify that cross-CA as a subscriber to that cross-certification certificate.

---

[451] Utah Code Ann. § 46-3-502(1).

[452] Utah Code Ann. § 46-3-502(1).

[453] Utah Code Ann. § 46-3-502(2)(a)(ii).

[454] Utah Code Ann. § 46-3-502(2).

[455] Utah Code Ann. § 46-3-304(4)(a).

[456] Utah Code Ann. § 46-3-304(4).

One obligation that cannot be waived under the Utah Act is the fiduciary obligation. The Act provides that if a CA holds the private key corresponding to the public key listed in the certificate it has issued, the CA hold the private key as a fiduciary of the subscriber named in the certificate.[457] Because fiduciary obligations in general cannot be waived, such activity carries a high risk of liability.

5.2.7 Effect of Consumer Statutes on Warranties and Limitations on Liability

At least initially, the CA plans to limit its certificate issuance to banks. Yet, because many of the relying parties will be consumers, the CA should consider the applicability of various consumer statutes to its CA activities.

One of the primary statutes the CA should consider is the federal Magnuson-Moss Warranty Act,[458] which applies to any warrantor who warrants a consumer product to a consumer through a written warranty.[459] Under the Magnuson-Moss Act, implied warranties cannot be disclaimed. If the written warranty is characterized as a "limited warranty," however, the implied warranties can at least be limited to the duration of the written warranty. The first issue to be determined, then, is whether bankers acquiring digital certificates fall within the definition of the terms above. For instance, the Act defines a "consumer product" as "any tangible personal property which is distributed in commerce and which is normally used for personal, family, or household purposes (including any such property intended to be attached to or installed in any real property without regard to whether it is so attached or installed."[460] A "consumer" means a buyer of any consumer product, any person *to whom the product is transferred* during the duration of the implied or written warranty or service contract, and any other person who is entitled under the terms of the warranty/service contract or under applicable State law to enforce the warranty/service contract against the warrantor/service contractor.[461] Thus, even a person who buys a product only for business purposes may qualify as a "consumer" if he is buying a consumer product. The term, however, does not include someone who buys for resale purposes. Id.

If the Magnuson-Moss Warranty Act does apply, its requirements must be strictly followed (particularly with disclaimers and other limitations, which must follow prescribed statutory language). Comparable state consumer protection laws exist, and, in most cases, they impose more restrictions and greater liability for violations than those associated with the Magnuson-Moss Act.

Consumer deceptive trade practices legislation could also apply to fraudulent misrepresentations by a CA. For example, the essential elements under Illinois law are: (1) a

---

[457] Utah Code Ann. § 46-3-305(3).

[458] 15 U.S.C. §§ 2301-2312.

[459] 15 U.S.C. § 2302(a) (1982).

[460] 15 U.S.C. § 2301(1) (1982).

[461] 15 U.S.C. § 2301(3) (1982).

deceptive act or practice including concealment or omission of any material fact, (2) defendant's intent that the plaintiff rely on the concealment, and (3) the concealment occurred in the course of conduct involving trade or commerce.[462]

A detailed examination of consumer protection law is beyond the scope of the memorandum. Nevertheless, the CA should be aware that there is a chance -- however remote -- that some of its conduct may fall under a consumer protection statute.

5.3 What Rules Apply to Contracts for Services?

As indicated earlier, the second legal tradition regarding contracts stems from the common law, including cases on licenses, service contracts, and information contracts, while a third legal tradition comes from the area of contracts dealing with informational content and essentially disallows implied obligations of accuracy or otherwise in reference to information transferred outside of a special relationship of reliance. Although courts are free to reason by analogy to the UCC[463] when construing a contract for services or information, there is no guarantee that a court will do so. Instead, a court could merely apply the common law in addition to any applicable standards of care that seem appropriate.

Generally, however, in analyzing service and information-oriented contracts, courts are more process-oriented (as opposed to result-oriented, as with goods) and thus tend to focus on how the contract is performed. Thus, the obligations of the service or information provider are to perform in a reasonably careful and workmanlike manner. When a company represents itself as capable of doing work of a particular character, a *warranty is implied* that the work will be *performed properly* or in a *workmanlike manner*.[464] This standard, in turn, is informed by the trade or profession from which the service provider comes.[465]

Because of this process-oriented emphasis, courts are reluctant -- in the absence of express language -- to construe contracts for professional services as implying a contract of guaranty or insurance of favorable results.[466] One reason for this reluctance is that persons providing professional services often must deal with factors beyond their control and thus they cannot be said to "insure favorable results" as a matter of common dealing.[467] (See discussion in this Section 5 regarding alarm companies, who make clear in their contracts that they are not insurers of results.) This would certainly be true of a CA, who, despite adherence to its stated procedures, issues an erroneous certificate.

---

[462] *White & Brewer Trucking, Inc. v. Donley,* 952 F. Supp. 1306, 1317-1318 (C.D. Ill. 1997).

[463] *See, e.g., Employers Ins. of Wausau v. Suwannee River SPA Lines, Inc.,* 866 F.2d 752, 765, n.25 (5th Cir. 1989) (where court observed, in evaluating a contract for services, that courts are free to reason by analogy to UCC § 2-316(1), which governs exclusion or modification of warranties.

[464] *Crank v. Firestone Tire & Rubber Co.,* 692 S.W.2d 397 (Mo.App. 1985).

[465] *Restatement (Second) of Torts,* § 299A.

[466] *Chemical Bank v. Title Services, Inc.,* 708 F. Supp. 245, 247 (D.Minn. 1989).

[467] *Chemical Bank v. Title Services, Inc.,* 708 F. Supp. 245, 247 (D.Minn. 1989).

In fact, when courts in various jurisdictions have purportedly applied an implied warranty of fitness to transactions that in essence contemplated the rendition of services, what was actually imposed was usually no more than a "warranty" that the service provider would not act negligently, a warranty of workmanlike performance imposing only the degree of care and skill that a reasonably prudent, skilled and qualified person would have exercised under the circumstances, or an implied warranty of competence and ability ordinarily possessed by those in the profession.[468]

In general, "those who hire experts for the predominant purpose of rendering services, relying on their special skills, cannot expect infallibility. Reasonable expectations, not perfect results in the face of any and all contingencies, will be ensured under a traditional negligence standard of conduct. In other words, unless the parties have contractually bound themselves to a higher standard of performance, reasonable care and competence owed generally by practitioners in the particular trade or profession defines the limits of an injured party's justifiable demands."[469]

Because services are judged by process, not by the results as the UCC would dictate, "the express warranty section would be no more applicable to a service contract than the [UCC's] implied warranty provisions."[470] Where the party rendering services can be shown to have expressly bound itself to the accomplishment of a *particular result,* however, the courts generally will enforce that promise.[471] Moreover, courts have recognized that parties in a commercial context may allocate risk for a defect in performance (just as parties allocate risk under the UCC for a defect in the product itself), with the contract price turning in part on whether the provider of services is willing to *guarantee* that is performance of the contract will be satisfactory.[472]

For example, cases examining the liability of title examiners have generally held that "'abstractors are free from an implied agreement of guaranty in the preparation of abstracts, particularly where the service consists only in searching records for instruments affecting title,'" even though the service does not involve unknown or uncontrollable factors.[473] Instead, courts focus on the *process* or *procedure* in assessing liability -- i.e., would a reasonable searcher find the financial statement or be put on notice to inquire elsewhere about it? In this regard, professional searchers can be charged with knowledge of standard practices used by filing clerks in indexing financial statements and be required to take these practices into account in requesting a search. A searcher could also have a duty to search under a variable spelling of the debtor's name if the spelling is commonly used by the debtor in conducting its affairs. Thus, if the searcher is adhering to accepted industry procedures (assuming they are commercially reasonable), a court is unlikely to find liability for errors. Likewise, courts could similarly assess

---

[468] *Milau Associates v. North Ave. Development,* 368 N.E.2d 1247, 1251 (N.Y. 1977).

[469] *Milau Associates v. North Ave. Development,* 368 N.E.2d 1247, 1250 (N.Y. 1977).

[470] *Milau Associates v. North Ave. Development,* 368 N.E.2d 1247, 1250 (N.Y. 1977).

[471] *Milau Associates v. North Ave. Development,* 368 N.E.2d 1247, 1250 (N.Y. 1977).

[472] *Employers Insurance of Wausau v. Suwannee River SPA ,* 866 F.2d 752, 765 (5th Cir. 1989)

[473] *Chemical Bank v. Title Services, Inc.,* 708 F. Supp. 245, 248 (D.Minn. 1989).

the liability of CAs, whose issuance of a certificate implies at least that a certain minimum procedure was followed.

In the title search cases, courts have also considered the policy considerations behind the notice filing system, which was to "create a simple system to provide reliable basic information to third persons without unduly burdening secured creditors."[474] Generally, the filing clerk is not required to engage in second-guessing (i.e., search for all possible misspellings of a creditor's name).[475] Just as the burden is on the creditors to make proper filings (who also bear the risk of misfiling), the burden should be on the subscribers to examine and accept the CA's certificate upon issuance to ensure its accuracy; the CA can help to ensure this through its contract with the subscriber, including appropriate indemnification clauses and/or by being licensed as a CA under a state digital signatures statute such as Utah's that imposes a duty on the subscriber to so act.

Courts have likewise been reluctant to convert alarm companies into insurers or guarantors of perfect performance. (See discussion in this Section 5 regarding alarm companies). The same can be said for contracts involving the provision of information.

If the CA's certification activity can be characterized as a license, sale, or other contract for *information*, the typical sale-of-goods law and the implied warranty of merchantability may well not apply.[476] Instead, common law contract principles and cases that consider free speech and other comparable noncommercial limitations on contractual obligations could well apply.

As discussed in Section 4, the *Restatement (Second) of Torts* regarding negligent misrepresentation provides a framework for assessing the obligations of information providers:

> One who, in the cause of his business, profession or employment, or in any other transactions in which he has a pecuniary interest, supplies false information for the guidance of others in their business transactions, is subject to liability for pecuniary loss caused to them by their justifiable reliance on the information, if he fails to exercise reasonable care or competence in obtaining or communicating the information.[477]

Even where a duty to users of information exists (as it arguably does with regard to the information provided by a CA to a relying party (even when it supplied indirectly through the subscriber), courts have upheld contractual disclaimers of accuracy in the information supplied.

For example, in *Rosenstein v. Standard & Poor's Corp,.*[478] S&P contracted with the Chicago Board Options Exchange (CBOE) to be the sole and exclusive source of data and summary index figures used for trading securities options. S&P contracted with Automated Data

---

[474] *Chemical Bank v. Title Services, Inc.,* 708 F. Supp. 245, 249 (D.Minn. 1989).

[475] *Chemical Bank v. Title Services, Inc.,* 708 F. Supp. 245, 249 (D.Minn. 1989).

[476] Raymond T. Nimmer, *Information Law,* § 12.14[2], at 12-59.

[477] *Restatement (Second) of Torts,* § 552.

[478] *Rosenstein v. Standard & Poor's Corp.,* 636 N.E.2d 665 (1st Dist. Ill. 1993).

Processing (ADP) to compute the indexes based on price information received from the New York Stock Exchange. The plaintiff who sought to recover (both his losses and those of the putative class members holding option contracts) against S&P claimed that ADP failed to timely correct inaccurate information provided by the NYSE late one Friday afternoon; the NYSE had corrected the error in three minutes and notified ADP, but ADP failed to make the correction until the following Monday, thereby resulting in the plaintiff losing considerable amounts of money. Although the court held that S&P did owe a duty to the plaintiff, that plaintiff did rely on S&P's representation, and that plaintiff was a member of a limited class that might have been foreseeable to S&P, the court found no liability because of a disclaimer in the agreement between S&P and the CBOE.[479] The disclaimer provided that "S&P shall obtain information for . . . use in the calculation of the S&P Indexes from sources which S&P considers reliable, but S&P does not guarantee the accuracy and/or the completeness of any of the S&P Indexes or any data included therein."[480] Although the plaintiff (the relying party) was not a direct party to this agreement, the license terms were incorporated into the rules of the CBOE (as required in the disclaimer clause in the agreement between S&P and the CBOE) and therefore governed the plaintiff's transactions.

In *Gale v. Value Line, Inc.,*[481] where the defendant had available the correct information but failed to publish it, the court emphasized that the defendant had never assumed responsibility in its solicitations for 100% accuracy, nor had it provided any assurances or guarantees, regarding the information it published in its newsletter that ranked convertible securities and included purchase recommendations. Thus, although the defendant's disclaimer failed (because it failed to protect itself from its own errors), the defendant incurred no liability because there was no expressed contract to be breached and no implied warranties arose.

In *McClure Engineering Associates, Inc. v. Reuben Donnelley,*[482] the Illinois Supreme Court upheld an exculpatory clause where the defendant was the publisher of a telephone directory who failed to publish a listing pursuant to an executed contract. The dissent in that case argued that the publisher of the telephone directory was the equivalent of a semipublic figure (a protected monopoly service with no competing company and no competing directory) and thus should be held liable.[483] The *Rosenstein* court distinguished the *McClure* dissent, emphasizing that the Rosenstein plaintiff made "*a conscious decision* to invest his money in the trading of options *subject to the exculpatory clause* which is a part of the CBOE Licensing Agreement and Rules." (See above discussion in this Section 5 regarding exculpatory contracts, where courts have enforced releases against plaintiffs who voluntarily chose to assume the risks of the activity subject to exculpatory clauses.) Likewise, parties relying on CA certificates

---

[479] *Rosenstein v. Standard & Poor's Corp.,* 636 N.E.2d 665 (1st Dist. Ill. 1993). *But see Lockwood v. Standard & Poor's Corp.,* 682 N.E.2d 131 (1st Dist. Ill. 1997) (finding plaintiff investors didn't even have standing to sue because they did not qualify as third-party beneficiaries under New York law).

[480] *Rosenstein v. Standard & Poor's Corp.,* 636 N.E.2d 665, 666 (1st Dist. Ill. 1993).

[481] *Gale v. Value Line, Inc.,* 640 F.Supp. 967 (D.R.I. 1986).

[482] 428 N.E.2d 1151 (Ill. 1981).

[483] The CA is entering a new field where there are not yet many CAs, but it would be hard to argue that it is a semipublic figure or that it is a protected monopoly. Thus, it is unlikely that the semipublic factor would constitute a basis for a special relationship that would shift obligations with respect to the services the CA would be providing.

would be making conscious decisions to engage in financial transactions through the subscriber (pursuant to an agreement between the subscriber and the relying party). If the CA includes the proper exculpatory provisions in its agreements with subscribers, and contractually requires subscribers to subject relying parties to such limitations, the CA could significantly decrease its scope of liability, at least with regard to negligence-related claims.

Thus, information providers generally are held not to warrant or commit to produce an accurate result in their contracts unless they expressly undertake to do so. It is not exactly clear, however, whether the very nature of a digital certificate may somehow imply some minimum level of accuracy. Although the CA's ability to limit is liability may vary from jurisdiction to jurisdiction,[484] if it avoids making promises of a particular result in its contracts and notices, and expressly disclaims liability for its own negligence, it should be able to reduce its liability risk.

[484] Some courts have permitted recovery of consequential damages in cases of breach of warranty in the performance of a service. *See, e.g., Crank v. Firestone Tire & Rubber Co.,* 692 S.W.2d 397, 403 (Mo.App. 1985) (analogizing to the UCC) (although damages for mere inconvenience cannot be recovered, if the inconvenience is coupled with a compensable element of damage, the plaintiff can recover for inconvenience caused by the breach where it is supported by evidence and shown with reasonable certainty).[484]

6. STATUTORY LIABILITY -- DIGITAL SIGNATURE REGULATION

One potential source of liability for the CA may arise through statute, specifically, from the application of provisions contained in digital signature legislation, and administrative regulations, promulgated under such statutes. Such regulation exists, or may soon exist, not only in the various states, but also at the federal and international levels.

6.1 State Legislation

Some form of digital or electronic signature legislation now has been passed or is being considered in 43 states[485]. Of these states, 9 have enacted or are currently considering comprehensive digital signature acts that embrace the concept of a certification authority and specifically address liability. Most of these acts are based substantially on the Utah/Washington model which is discussed in detail below. Other less comprehensive acts expressly authorize the use of digital or electronic signatures either generally or in connection with communications with public entities but may or may not expressly contemplate the use of certification authorities or specifically address liability. Still others merely authorize the use of digital or electronic signatures in connection with a specific context, such as filing tax returns or corporate documents with the state government, and do not specifically address certification authorities or their liability. It is difficult to predict how many of these statutes, or regulations to be adopted thereunder, could affect CA liability.

6.1.1 The Utah/Washington Model

The Utah Digital Signature Act (the "Utah Act")[486] was the first comprehensive digital signature act to be enacted. It creates a litany of potential statutory liability for certification authorities as well as for subscribers and repositories. On the other hand, the Utah Act also helps to *limit* the amount of potential liability in some ways too.

The Washington Electronic Authentication Act (the "Washington Act," and together with the Utah Act, the "Utah/Washington Model") was enacted soon after enactment of the Utah Act and mirrors the Utah Act in most respects.[487] There are a few differences worth mentioning, however, most of which are the result of amendments made to the Washington Act early in 1997 prior to the Act becoming effective. Since enactment of the Utah and Washington acts, other states have followed suit and have enacted[488] or are currently considering[489] legislation substantially based on the Utah/Washington Model.

---

[485] A summary of all pending and enacted electronic signature and digital signature legislation, at the state, federal, and international level, is maintained (and updated weekly) on our web site at ***www.bakernet.com/ecommerce***.

[486] Utah Code Ann. §§ 46-3-101 to -504. *See also* Utah Admin. R. 154-10-100 to -501 (regulations pertaining thereto).

[487] Wash. Rev. Code Ann. §§ 19.34.010 to .903.

[488] The Minnesota Electronic Authentication Act was enacted in May of 1997. Minn. Stat. Ann. §§ 325K.001 to .26 (requires that effect be given to contractual liability allocations between parties, but does not expressly release CAs and repositories from liability in excess of recommended reliance limits or from certain kinds of damages). Except for the significant deviation noted in brackets, it is substantially similar to the Utah/Washington Model.

What follows is a summary of the various ways in which the Utah Act, and state acts modeled after it, may give rise to potential statutory liability for the CA in issuing certificates and performing services related thereto. Relevant portions of the Utah Act are set forth below. Material differences between the Utah Act and the Washington Act are pointed out in the footnotes. Most, but not all, of the obligations imposed on a CA imply only to licensed CAs. Becoming a licensed CA is optional.

(a) Specific Duties and Obligations

The Utah Act imposes upon CAs, subscribers and repositories certain specific duties and obligations. For CAs, these obligations generally relate to the issuance and revocation of certificates. For example, in issuing a certificate a licensed CA must confirm various details including that the prospective subscriber is the person to be listed in the certificate, that the prospective subscriber rightfully holds the private key to be listed in the certificate and that the information in the certificate is accurate after due diligence.[490] Satisfaction of this requirement cannot be waived or disclaimed by the CA or the subscriber.[491] With respect to revocation, licensed CAs must undertake to revoke certificates in a timely fashion (within one day) upon receiving a confirmed request for revocation.[492] The Utah Act also imposes upon licensed CAs certain responsibilities with respect to using only a trustworthy system and disclosing its certification practice statement.[493]

Failure on behalf of licensed CAs to comply with these and other statutory requirements could have various consequences. For example, noncompliance could result in an investigation by the Division of Corporations and Commercial Code within the Utah Department of Commerce, the agency responsible for carrying out the purpose of the Utah Act (the "Division"), and eventually in prosecution or civil enforcement by the Division.[494] This investigation could lead to possible licensing restrictions or license revocation or suspension, and the CA could be ordered to pay the costs incurred by the Division in enforcing the Utah Act.[495] Furthermore, persons who knowingly or intentionally violate a Division order may be subject to a civil penalty

---

[489] The following state bills are currently under consideration and are substantially similar to the Utah/Washington Model, except for the significant deviations noted in brackets: 1997 Haw. Senate Bill 961 (would permit punitive damages against CAs whose noncompliance with agency order causes injury; would impose a forty year record-keeping requirement; CA must pay reasonable restitution to subscriber for interruption to business due to revocation of unreliable certificate); 1997 Mich. Senate Bill 204; 1998 Mo. House Bill 1126 (1998 Mo. Senate Bill 708 is substantially identical); 1997 New York Senate Bill 2238 (1997 New York Assembly Bill 6183 is substantially identical); 1997 Rhode Island Senate Bill 612; 1997 Vt. Senate Bill 206 (1997 Vt. House Bill 60 is substantially identical).

[490] Utah Code Ann. § 46-3-302(1).

[491] Utah Code Ann. § 46-3-302(1)(c).

[492] Utah Code Ann. § 46-3-307(2).

[493] Utah Code Ann. § 46-3-301.

[494] Utah Code Ann. § 46-3-203.

[495] Utah Code Ann. § 46-3-203(4), (5).

of not more than $5,000 per violation or 90% of the recommended reliance limit of a material certificate, whichever is less.[496]

Licensed or unlicensed, CAs who conduct their business in a manner that creates "an unreasonable risk of loss" to subscribers, relying parties or repositories could be subject to injunctive or other civil relief as requested by the Division (though no private right of action with respect to this provision exists at this time) under the Utah Act.[497] What constitutes an unreasonable risk of loss is not defined by the Utah Act or the regulations; nor is there any case law on the subject. Nevertheless, a concern is that this provision could subject a CA licensed in another state (or not licensed in any state) to potential liability in Utah, provided that Utah has a sufficient basis for extending jurisdiction such as by, for example, the presence of a relying party in the state.

In addition to the administrative enforcement concerns, these statutory liability provisions potentially could also serve as the basis for common law negligence, misrepresentation and various other tort claims which are discussed in more detail in Section 4 above.

(b) Warranty Liability

A CA licensed under the Utah Act is deemed to make certain statutory warranties to subscribers upon issuing a certificate. Included in these warranties is that the certificate contains no information known to the CA to be false, that the certificate satisfies all material requirements of the Utah Act, and that the CA has not exceeded any limits of its license in issuing the certificate.[498] The Utah Act prohibits the CA from disclaiming or limiting these warranties.[499]

A licensed CA is also deemed to make various statutory representations upon issuing a certificate. As to the subscriber, unless agreed otherwise, the CA represents that it will act promptly to suspend or revoke a certificate and that it will notify the subscriber within a reasonable time of any facts known to the CA which significantly affect the validity or reliability of the certificate.[500] As to all parties who reasonably rely on the certificate, the CA certifies that the information in the certificate and listed as confirmed by the CA is accurate, that all foreseeable information material to the reliability of the certificate is stated or incorporated by reference, that the subscriber has accepted the certificate, and that the CA has complied with all applicable laws of Utah governing the issuance of the certificate.[501]

---

[496] Utah Code Ann. § 46-3-203(3). The Washington Act differs from the Utah Act here in several ways. First, in Washington the imposition of a civil penalty is not necessarily contingent upon a "knowing or intentional" violation of an administrative order. Second, it provides for a maximum penalty of $10,000 (rather than $5,000). Finally, in case of a violation continuing for more than one day, each day is considered a separate incident. RCW § 19.34.120(3). For a list of the criteria used to determine penalty amounts in Washington, *see* WAC 434-180-270.

[497] Utah Code Ann. § 46-3-204.

[498] Utah Code Ann. § 46-3-303(1)(a).

[499] Utah Code Ann. § 46-3-303(1)(b).

[500] Utah Code Ann. § 46-3-303(2).

[501] Utah Code Ann. § 46-3-302(3).

Though these warranties and representations are unlikely to give rise to statutory liability *per se,* they most likely could give rise to potential liability based on common law actions for breach of warranty and misrepresentation. In such disputes the statute itself will serve to establish the various warranties and representations that were made to subscribers and relying parties. Thus, parties suing a CA on these grounds will most likely have a much easier time establishing their case given that the one of the elements they have to show (arguably the most difficult element for plaintiffs to show otherwise) has already been established by operation of the statute.

Cutting against this potential liability, however, is the fact that upon accepting a certificate subscribers undertake to indemnify the issuing CA for loss or damage caused by an intentional or negligent material misrepresentation or failure to disclose.[502] This indemnification on behalf of subscribers may not be contractually disclaimed or limited in scope.[503] Of course in many cases subscribers may not have the wherewithal to indemnify their CAs in the event of loss. However, given that the CA plans to deal exclusively with banks, the indemnification provision could serve to eliminate or at least reduce some of the CA's out-of-pocket losses.

(c) Acknowledgment Liability

Section 405 states that "[u]nless otherwise provided by law or contract, a certificate issued by a licensed certification authority is an acknowledgment of a digital signature . . . regardless of whether words of an express acknowledgment appear . . . ."[504] This provision might be construed as placing the CA in the position of a notary public thereby subjecting the CA to potential notarial liability with respect to the acknowledgment of documents. Indeed, this potential for liability has already been expressly recognized in the Washington Act, as amended.[505]

(d) Control of the Private Key

The Utah Act provides that if the CA holds the private key corresponding to the public key listed in a certificate which it has issued, the CA holds the private key as a fiduciary of the subscriber named in the certificate and may use that private key only with the subscriber's prior written approval, unless agreed otherwise.[506] For CAs who hold private keys for their

---

[502] Utah Code Ann. § 46-3-304(4)(a).

[503] Utah Code Ann. § 46-3-304(4)(b).

[504] Utah Code Ann. § 46-3-405. The Washington Act, on the other hand, does not make the issuance of a certificate an acknowledgment by default. Instead a certificate constitutes an acknowledgment only "if so provided in the certificate" and "if words of an express acknowledgment appear with the digital signature." RCW § 19.34.340(1). Moreover, the Washington Act expressly recognizes that "If the digital signature is used as an acknowledgment, then the certificate authority is responsible to the same extent as a notary up to the recommended reliance limit for failure to satisfy the requirements for an acknowledgment."

[505] The Washington Act expressly recognizes that "If the digital signature is used as an acknowledgment, then the certificate authority is responsible to the same extent as a notary up to the recommended reliance limit for failure to satisfy the requirements for an acknowledgment." RCW § 19.34.340(2).

[506] Utah Code Ann. § 46-3-305(3). The Washington Act, as amended, no longer contains this provision. RCW § 19.34.240. Moreover, a recently proposed amendment to the Minnesota Electronic Authentication Act would

subscribers, this provision would appear to give rise to potential breach of fiduciary duty claims in the event a private key in their possession is misused or compromised. Moreover, since the private key is deemed to be the personal property of the subscriber who rightfully holds it,[507] holding subscribers' private keys could also give rise to a bailee-bailor relationship and potential liability therefrom. Since the CA does not intend to hold the private keys of its subscribers, however, these potential sources of liability should not cause great concern.

Potential fiduciary and bailee liability is not the only risk to CAs associated with handling private key. It must not be overlooked that to the extent a CA acts as a subscriber in a transaction (e.g., chain certification of a CA-issued certificate), the CA assumes a statutory duty as a subscriber to exercise reasonable care to retain control of the private key and prevent its disclosure to any person not authorized to create the CAs digital signature.[508] This duty of care is, of course, in addition to any duty of care on behalf of the CA that most likely exists under negligence law to retain control over the CA's private key, whether or not the CA has its certificate chain-certified.

(e) Judicial Presumptions

The Utah Act provides that in adjudicating a dispute involving a digital signature, Utah courts shall presume that "a certificate digitally signed by a licensed certification authority and either published in a recognized repository or made available by the issuing certification authority or by the subscriber listed in the certificate is issued by the certification authority which digitally signed it . . . ."[509] This creates a rather strong presumption that may be difficult to rebut. Should a CA employee erroneously issue a certificate, or issue a certificate without authorization, this provision would presume that the certificate was issued by the CA.

(f) Record-keeping Requirements

The Utah Digital Signature Administrative Rules (the "Utah Rules") impose upon licensed CAs certain record-keeping requirements. CAs are required to maintain documentation of compliance with the Utah Act and to retain its records regarding the issuance, acceptance and any suspension or revocation of a certificate for at least ten years after the certificate is revoked or expires.[510] Moreover, the Utah Rules also require that CAs themselves retain the records, unless turned over to the Division or a succeeding licensed CA.[511]

---

expressly prohibit a CA from holding a private key on behalf of a subscriber. 1997 Minn. Senate Bill 2068 (introduced January 20, 1998).

[507] Utah Code Ann. § 46-3-305(2). *But see* 1997 Minn. Senate Bill 2068 (would repeal this provision).

[508] Utah Code Ann. § 46-3-305(1).

[509] Utah Code Ann. § 46-3-406(1).

[510] Utah Admin. R. 154-10-303.

[511] Utah Admin. R. 154-10-303(5).

The consequence of failing to comply with this rule is not specified, but presumably the Division can enforce compliance just as it would with any other violation of the Utah Act, through investigation and prosecution or civil enforcement.

(g) Cessation of Certification Authority Activities

Utah Rule 154-10-304 imposes upon CAs a duty to give subscribers of unrevoked or unexpired certificates at least 90 days written notice before ceasing to act as a CA and to pay reasonable restitution to subscribers for revoking such unexpired certificates. These requirements may be modified by contract, provided that the CA must always give at least ten days written notice before ceasing to act as a CA.[512] Moreover, CAs must give written notice to the Division at least two months prior to ceasing to act as CA.[513]

(h) Repository Liability

It also must be recognized that the CA may find itself wearing many hats throughout the course of its performance of certification authority services. For example, to the extent the CA serves as a repository for publishing the certificates it issues, for posting notices of suspended or revoked certificates and for posting certification authority disclosure records, it will be subject to the liability provisions concerning repositories. These liability provisions provide that "a repository is liable for a loss incurred by a person reasonably relying on a digital signature verified by the public key listed in a suspended or revoked certificate if: (a) the loss was incurred more than one business day after receipt by the repository of a request to publish notice of the suspension or revocation; and (b) the repository had failed to publish the notice of suspension or revocation when the person relied on the digital signature."[514] This potential liability on the part of a repository cannot be disclaimed by contract.[515]

The Utah Act does attempt to shelter a *recognized* repository from liability for certain events, however, including misrepresentation in a certificate published by a licensed CA, for accurately reporting information which licensed CAs have published, for reporting information about a CA, a certificate or a subscriber (if the information is published in accordance with the Utah Act and regulations) and for failure to publish notice of a suspension or revocation so long as one business day has not elapsed since the notice was received.[516] The Utah Act also limits the amount of damages to the amount specified in the certificate as the recommended reliance limit,[517] and provides that a *recognized* repository is liable only for "direct compensatory

[512] Utah Admin. R. 154-10-304(3).

[513] Utah Admin. R. 154-10-304(4).

[514] Utah Code Ann. § 46-3-502(1).

[515] Utah Code Ann. § 46-3-502(1).

[516] Utah Code Ann. § 46-3-502(2).

[517] Utah Code Ann. § 46-3-502(2)(a)(ii).

damages, which do not include: (i) punitive or exemplary damages; (ii) damages for lost profits, savings, or opportunity; or (iii) damages for pain and suffering."[518]

(i) Subscriber Liability

Another hat the CA may wear is that of a subscriber to certificates issued through cross-certification or by a higher-level CA. To the extent a CA acts as a subscriber to a certificate, that CA is deemed to make certain statutory representations as a subscriber to persons who reasonably rely on the information contained in the certificate. Namely, by accepting a certificate, the subscriber listed in the certificate certifies that it rightfully holds the private key listed in the certificate and that all representations made to the CA and material to information listed in the certificate are true.[519] These representations may not be disclaimed or contractually limited if the disclaimer or limitation restricts liability for misrepresentation as against persons reasonably relying on the certificate.[520] Thus when the CA acts as a subscriber to certificates issued by another CA these statutory representations will apply and could serve as the basis for a misrepresentation claim by a relying party.

(j) Potential Limits of Liability Under the Utah Act

Despite the various provisions contained in the Utah Act that may give rise to potential statutory liability, the Utah Act also provides for various means by which a CA can endeavor to limit or reduce its liability.

Recommended Reliance Limits. The Utah Act endeavors to limit a licensed CA's exposure to liability by permitting the use of recommended reliance limits. By specifying a recommended reliance limit in a certificate, CAs "recommend that persons rely on the certificate only to the extent that the total amount at risk does not exceed the recommended reliance limit."[521] The real benefit of this provision, however, is that a licensed CA is "not liable in excess of the amount specified in the certificate as its recommended reliance limit for either: (i) a loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed certification authority is required to confirm; or (ii) failure to comply with [the CA's statutory duties and obligations] in issuing the certificate."[522]

Types of Damages. The Utah Act also expressly limits the types of damages available to injured relying parties. Licensed CAs are liable only for "direct, compensatory damages in any

---

[518] Utah Code Ann. § 46-3-502(2)(b). The Washington Act provides that a recognized repository is not liable for "(i) Punitive or exemplary damages; or (ii) Damages for pain and suffering." RCW § 19.34.410(2)(c). Moreover, the Washington Act provides that "Consequential or incidental damages may be liquidated, or may otherwise be limited, altered, or excluded unless the limitation, alteration, or exclusion is unconscionable." A recognized repository may accomplish this either by agreement or by notifying any relying party prior to reliance. RCW § 19.34.410(3).

[519] Utah Code Ann. § 46-3-304(1).

[520] Utah Code Ann. § 46-3-304(3).

[521] Utah Code Ann. § 46-3-309(1).

[522] Utah Code Ann. § 46-3-309(2)(b)

action to recover a loss due to reliance on the certificate, which damages do not include: (i) punitive or exemplary damages; (ii) damages for lost profits, saving, or opportunity; or (iii) damages for pain or suffering."[523]

Of course these liability limits do not apply to *unlicensed* CAs.[524] But Utah does recognize these liability limits with respect to CAs licensed in other states so long as those licensing requirements are substantially similar to those of Utah.[525]

Compliance with the Provisions of the Act. Complying with the provisions of the Utah Act has its benefits aside from reducing the risk of exposure to common law claims for negligence, breach of warranty, misrepresentation, etc. Most notably, the Utah Act provides that a CA is "not liable for any loss caused by reliance on a false or forged digital signature or a subscriber, if, with respect to the false or forged digital signature, the certification authority complied with all material requirements of [the Utah Act]" unless the CA waives this provision.[526]

Presumptions of Identity. The Utah Rules also help to cut against potential liability for licensed CAs in at least one significant way. Rule 154-10-303(2) provides that the identification of a person or entity named in a certificate "shall be presumed to be established" where a licensed certification authority has been presented with at least one of a list of government issued or government recognized IDs, including a birth certificate, driver's license or state ID card. This provision seems to provide somewhat of a safe harbor for CAs to rely on these forms of ID, provided of course that such reliance is reasonable under the circumstances.

Reasonableness of Reliance. "Unless otherwise required by law or contract, the recipient of a digital signature assumes the risk that a digital signature is forged, if reliance on the digital signature is not reasonable under the circumstances."[527] This provision would appear to help reduce a CA's liability by placing at least some duty of care upon relying parties.

---

[523] Utah Code Ann. § 46-3-309(2)(c). The Washington Act has modified this language somewhat to read that a licensed CA is "not liable for: (i) Punitive or exemplary damages . . . or (ii) Damages for pain and suffering." RCW § 19.34.280(2)(c). Moreover, the Washington Act provides that "Consequential or incidental damages may be liquidated, or may otherwise be limited, altered, or excluded unless the limitation, alteration, or exclusion is unconscionable." A licensed CA may accomplish this either by agreement or by notifying any relying party prior to reliance on the certificate. RCW § 19.34.280(4).

[524] Utah Code Ann. § 46-3-201(6). Note that the Division may limit the scope of a CA's license by imposing specified limitations with respect to the maximum number of outstanding certificates, the cumulative maximum of recommended reliance limits in certificates issued, or issuance only within a single firm or organization. Utah Code Ann. § 46-3-201(3)(a). A CA acts as an unlicensed CA to the extent it exceeds these license limitations. Utah Code Ann. § 46-3-201(3)(b). Rather than regarding the CA as being unlicensed in such cases, the Washington Act instead provides that the statutory limitations of liability do not apply. RCW § 19.34.100(3).

[525] Utah Code Ann. § 46-3-201(5).

[526] Utah Code Ann. § 46-3-309(2)(a). The Washington Act expressly provides that this subsection does not relieve a licensed CA of its liability for breach of any of the warranties or certifications it makes in connection with the issuance of a certificate or for its lack of good faith.

[527] Utah Code Ann. § 46-3-402.

6.1.2 Other State Models that Address CA Liability

The Utah/Washington Model discussed above is by far the most comprehensive model in terms of dealing with the liability of CAs and others. But state legislation based on the Utah/Washington model is by no means the only potential source of statutory liability specifically pertaining to the activities of a CA. Many states have enacted or are currently considering digital or electronic signature legislation, the effect of which on the CA's potential statutory liability is not yet clear. Furthermore, given the lack of consensus or uniform precedent, significant concern arises from the fact that it is impossible to predict the various theories for CA liability that states may employ. Undoubtedly there are new, imaginative models on the horizon that could potentially expose CAs to significant risk of liability. It should also be kept in mind that many states have authorized an administrative agency, usually the secretary of state or its functional equivalent, to issue regulations the final form and effect of which cannot be determined at this time.

What follows is a summary of some other state models that differ significantly from the Utah/Washington Model and their possible effect on CA liability.[528]

(a) California

Although the California electronic signature legislation adopted in 1995[529] neither expressly embraces the concept of a certification authority, nor specifically addresses liability, the proposed California regulations would. If adopted in their final draft form, the proposed California regulations would recognize that CAs may be used for the purpose of issuing certificates in connection with communications with public entities.[530] As to liability, the proposed California regulations would provide that "[w]hether a signature is accompanied by a certificate or note, the person who holds the key pair, or the subscriber identified in the certificate, assumes a duty to exercise reasonable care to retain control of the private key and prevent its disclosure to any person not authorized to create the subscriber's digital signature."

---

[528] The following discussion summarizes only those models that contemplate the role of private CAs and/or repositories and that specifically address liability issues. Models that limit the recognition of electronic signatures to communications with public entities, that only govern the use of a governmental agency as a CA, that do not specifically address potential liability or that apply only to the use of electronic or digital signatures in a limited context (such as filing documents with the state government) are not discussed. Such models, to the extent if any they would apply to the activities proposed to be conducted by the CA, do not provide much general guidance with respect to determining potential liability. To the extent the CA conducts activities specifically governed by these statutes it should take measures to ensure compliance these statutory requirements. For example, where a state government imposes certain specific requirements with respect to using digital or electronic signatures in connection with communications filed with state agencies, the CA would have to endeavor to comply with these requirements.

[529] Cal. Gov't Code § 16.5 (1995). The scope of the California legislation is limited to electronic communications with a "public entity" and does not apply generally to electronic communications between private parties.

[530] See Proposed Digital Signature Regulations for California (www.ss.ca.gov/digsig/digsig.htm); *see also* proposed Texas Digital Signature Regulations (www.state.tx.us/EC/digital_signature.htm) (substantially similar to proposed California regulations).

(b) Florida

Florida's Electronic Signature Act of 1996 (the "Florida Act") contemplates the use of CAs but does not specifically address their responsibilities or potential liability.[531] Florida House Bill 1413 (enacted May, 1997) authorizes the Secretary of State to establish a voluntary licensure program for private CAs and to make rules necessary to implement and enforce the program. It is too early to tell what the final regulations will look like, but the initial working draft contains some of the principals found in the Utah Act and Utah Regulations, such as imposing certain obligations upon CAs in connection with issuing and revoking certificates and establishing record-keeping and notice of cessation requirements.

(c) Georgia

The Georgia Electronic Records and Signatures Act (enacted) provides for the general use of electronic signatures, regardless of whether they are used in connection with public or private communications.[532] As to liability, the Act provides that "A person whose electronic signature is used in an unauthorized fashion may recover or obtain any or all of the following against the person who engaged in such unauthorized use, provided that the use of such electronic signature in an unauthorized fashion was negligent, reckless, or intentional: (1) Actual damages; (2) Equitable relief, including, but not limited to, an injunction or restitution of money or property; (3) Punitive damages under [certain] circumstances . . .; (4) Reasonable attorneys' fees and expenses; and (5) Any other relief which the court deems proper."[533]

(d) Illinois

The Illinois Electronic Commerce Security Act (the "Illinois Act") takes effect on July 1, 1999.[534]

(1) CA and Repository Duties

The Illinois Act expressly recognizes that persons are going to rely on certificates issued by CAs. Section 15-201 provides that "It is foreseeable that persons relying on a digital signature will also rely on a valid certificate containing the public key by which the digital signature can be verified, during the operational period of such certificate and within any limits specified in such certificate." Such an express acknowledgment appears to set the stage for potential negligence and fraud claims.

Section 15-305 imposes certain disclosure duties upon a CA. It provides that "In the event of an occurrence that materially and adversely affects a certification authority's operations or system, its certification authority certificate, or any other aspect of its ability to operate in a

---

[531] 1996 Fla. Senate Bill 942 (enacted).

[532] 1997 Ga. Senate Bill 103 (enacted).

[533] 1997 Ga. Senate Bill 103 § 10-12-4.

[534] Copies are available at ***www.bakernet.com/ecommerce***.

trustworthy manner, the certification authority must act in accordance with procedures governing such an occurrence specified in its certification practice statement, or in the absence of such procedures, must use reasonable efforts to notify any persons that the certification authority knows might foreseeably be damaged as a result of such occurrence."

Section 15-315 sets forth certain statutory representations that are deemed to be made by a CA upon issuing a certificate. Included in these representations are that: (1) the CA has processed, approved, and issued, and will manage and revoke if necessary, the certificate in accordance with its CPS or applicable law; (2) the CA has verified the identity of the subscriber to the extent stated in the certificate or its applicable certification practice statement, or in lieu thereof that the certification authority has verified the identity of the subscriber in a trustworthy manner; (3) the CA has verified that the person requesting the certificate holds the private key corresponding to the public key listed in the certificate; and (4) unless conspicuously disclaimed, to the CA's knowledge as of the date the certificate was issued, all other information in the certificate is accurate and not materially misleading. If the CA issued the certificate subject to the laws of another jurisdiction, the CA also is deemed to have made all warranties and representations, if any, otherwise applicable under law governing its issuance. Failure on behalf of a CA to comply with these representations could potentially give rise to claims of misrepresentation.

Section 15-320 imposes upon a CA certain duties pertaining to the revocation of certificates. Namely, a CA must revoke certificates in accordance with the policies and procedures set forth in its CPS or, in the absence of such policies and procedures, in accordance with the Act. Upon effecting a revocation, the CA has a duty to notify the subscriber and relying parties in accordance with the policies and procedures set forth in its CPS. In the absence of such policies and procedures, the CA must promptly notify the subscriber, promptly publish notice of the revocation in all repositories where the CA previously caused publication of the certificate, and otherwise disclose the fact of revocation on inquiry by a relying party. Noncompliance could give rise to negligence or misrepresentation.

Section 15-301 imposes upon CAs and repositories a duty to maintain their operations and perform their services in a trustworthy manner, unless conspicuously set forth otherwise in the CPS. "Trustworthy manner" requires "the use of computer hardware, software, and/or procedures that, in the context in which they are used: (a) can be shown to be reasonably resistant to penetration, compromise, and misuse; (b) provide a reasonable level of reliability and correct operation; (c) are reasonably suited to performing their intended functions or serving their intended purposes; (d) comply with applicable agreements between the parties, if any; and (e) adhere to generally accepted security procedures."[535]

(2) Restrictions on the Publication of Certificates

Section 15-205 prohibits a person from publishing a certificate, or knowingly making it available to anyone likely to rely on it, if such person knows that: (1) the CA listed in the

[535] Illinois Act § 5-105.

certificate has not issued it; (2) the subscriber listed in the certificate has not accepted it; or (3) the certificate has been revoked or suspended.

(3) Signer Liability

Section 10-125 of the Illinois Act imposes upon signers (and their authorized persons) a duty to exercise reasonable care to retain control and maintain secrecy of their "signature device" (which includes a private key) and to protect it from any unauthorized access, disclosure or use during the period when reliance on a signature created by the signature device is reasonable. In the event of a compromise, the signer or authorized person "must make a reasonable effort to promptly notify all persons that such person knows might foreseeably be damaged as a result of such compromise. . ."

Aside from potentially giving rise to negligence claims, the effect of failing to control access to one's private key is made explicit. Section 10-130 provides that a "secure electronic signature is attributable to the person to whom it correlates, whether or not authorized, if: (1) the electronic signature resulted from acts of a person that obtained the signature device or other information necessary to create the signature from a source under the control of the alleged signer, creating the appearance that it came from that party; (2) the access or use occurred under circumstances constituting a failure to exercise reasonable care by the alleged signer; and (3) the relying party relied reasonably and in good faith to its detriment on the apparent source of the electronic record."[536]

(4) Subscriber Liability

Section 20-101 provides that "All material representations knowingly made by a person to a CA for purposes of obtaining a certificate naming such person as a subscriber, must be accurate and complete to the best of such person's knowledge and belief."

Section 20-105 provides that by accepting a certificate, a subscriber represents to any person who reasonably relies on information contained in the certificate that: (1) the subscriber rightfully holds the private key corresponding to the public key listed in the certificate; (2) all representations made by the subscriber to the CA and material to the information listed in the certificate are true; and (3) all information in the certificate that is within the knowledge of the subscriber is true. Noncompliance could give rise to claims of misrepresentation.

A subscriber also undertakes a duty to promptly request revocation of a certificate, and to publish notice of the revocation or otherwise provide reasonable notice of the revocation, upon compromise of the private key.[537]

---

[536] An exception to such attribution applies to electronic transactions deemed to be consumer transactions. It does not appear to be often, however, that this exception would apply when the CA acts as a signer to its certificates.

[537] Illinois Act § 20-110.

(5) Intentional or Knowing Misconduct

The Illinois Act penalizes persons who knowingly or intentionally use the signature device of another person or a certificate in an unauthorized or fraudulent manner.[538] Similarly, persons are also expressly prohibited from knowingly misrepresenting their identity or authorization in requesting or accepting a certificate or in requesting suspension or revocation of a certificate.[539] Such persons are subject not only to criminal sanctions, but may also be liable for appropriate civil relief to persons who suffer loss by reason of their actions.[540]

6.2 Federal Legislation

Although no digital or electronic signature has yet been passed at the federal level, two bills are currently being considered. It is unclear at this time whether the final form of these bills, if passed, would preempt state legislation to any extent.

6.2.1 The Electronic Financial Services Efficiency Act of 1997

Currently being considered in Congress is the Electronic Financial Services Efficiency Act of 1997.[541] This Bill describes as one of its purposes to "define and harmonize the practices, customs, and uses applicable to the conduct of electronic authentication."[542] There has been some debate as to the extent to which, if any, the Bill would purport to preempt state legislation in this area.

This Bill would define "certification authority" as "any private or public entity which provides *assurance* that a particular digital signature, or other form of electronic authentication, is tied to the identity of an individual or legal entity, or *attests* to the current validity of such a signature."[543]

Perhaps most concerning to the CA is this Bill's intent to establish the National Association of Certification Authorities ("NACA").[544] The Bill would require that any person or group wishing to provide electronic authentication services in the United States would have to be a registered member of NACA, subject to NACA's authority to deny membership.[545]

---

[538] Illinois Act §§ 10-140, 15-210, 15-215, and 95-15.

[539] Illinois Act § 15-215.

[540] Illinois Act § 30-5.

[541] H.R. 2937, 105th Cong., 1st Sess. (1997).

[542] H.R. 2937 § 2(b). Note that Senator Robert F. Bennett (R-UT) has also expressed an intent to introduce legislation early this year to provide a uniform framework for the use of electronic authentication services.

[543] H.R. 2937 § 3(5) (emphasis added).

[544] H.R. 2937 § 7(a).

[545] H.R. 2937 §§ 7(b), (c).

The Electronic Authentications Standards Review Committee (the "Standards Review Committee") would be created under NACA to "establish, develop, and refine criteria to be applied to the emerging electronic authentication industry, including -- (A) the roles and responsibilities of the parties involved in electronic authentication; . . . (C) recognition of foreign legal and regulatory standards; and (D) transparency requirements, licensing, and registration of certification authorities."[546] The Standards Review Committee would also be charged with establishing and adopting "such guidelines, standards, and codes of conduct regarding the use of electronic authentication by members of [NACA], including the rights and responsibilities of certification authorities in matters involving notification, disclosure requirements, liability of consumers and certification authorities, and hearing procedures regarding disciplinary actions to be take by the Standards Review Committee . . . ."[547] Finally, the Standards Review Committee would be given "enforcement powers to ensure minimum standards and protections for consumers and shall establish and adopt disciplinary procedures and policies."[548] Violation of such guidelines, standards, or code of conduct could result in public censorship, suspension or prohibition from providing electronic authentication services in the United States and civil penalties.

With respect to consumer protection, the Bill would impose upon CAs a duty to notify as to the fact of the authentication of consumer transactions or communications.[549]

6.2.2 The Electronic Commerce Enhancement Act of 1997

The Electronic Commerce Enhancement Act of 1997,[550] if enacted in its current form, would among other things require the establishment of guidelines governing the acceptance of certificates by government agencies.[551] The guidelines would provide that agencies could only accept certificates issued by the agency itself or a "trusted third party" that is licensed or accredited either by a State or local government or an appropriate accreditation body.[552] Moreover, the guidelines would require that an agency could accept certificates "only from a trusted third party that, in accordance with commercially reasonable standards, accepts liability for and is insured against negligent issuance or handling of certificates."[553]

---

[546] H.R. 2937 § 7(e)(1).

[547] H.R. 2937 § 7(e)(2).

[548] H.R. 2937 § 7(e)(3).

[549] H.R. 2937 § 9(b).

[550] H.R. 2991, 105th Cong., 1st Sess. (1997).

[551] H.R. 2991 § 6(a).

[552] H.R. 2991 § 6(b).

[553] H.R. 2991 § 6(c).

6.2.3 The Secure Public Networks Act

The Secure Public Networks Act (otherwise known as the McCain/Kerrey Bill),[554] if approved in its current form, would for the first time impose domestic restrictions on the ability of American citizens to use encryption technologies inside the United States. The Bill would also create a voluntary registration system pursuant to which "any private person, entity, government entity, or foreign government agency" could register to act as a certification authority.[555]

6.3 International Legislation

Not only might state and federal digital signature regulation give rise to potential statutory liability, but also the possibility exists that international regulation may eventually give rise to potential statutory liability. Various foreign nations have already enacted or are currently considering bills pertaining to electronic and digital signatures and electronic commerce that might have an impact on the CA should it choose to issue certificates for use outside the United States.[556] Furthermore, potential liability under the laws of these countries is not necessarily limited to laws concerning digital signatures. Other laws imposing official language requirements or restrictions on the use of encryption technology may lead to potential violations and subsequent liability.

[554] S. 909, 105th Cong., 1st Sess. (1997).

[555] S. 909 § 402.

[556] *E.g.,* Argentina, Canada, Denmark, France, Germany, Italy, Japan, Malaysia, Sweden and the United Kingdom. The European Union is also working towards developing European legislation.

7. INTELLECTUAL PROPERTY LIABILITY

7.1 Overview

Intellectual property refers to a set of legally-recognized rights in intangible subject matter such as inventions and trademarks. These rights, discussed below in more detail, include patents, copyrights, trade secrets, and trademarks and related rights arising under unfair competition and privacy laws. Activities of a CA that violate intellectual property rights of another party are said to *infringe* the other party's rights. Depending upon the right infringed, remedies for infringement may include damages, profits, punitive damages, attorney fees and injunctions against further infringement.

7.2 Patents

7.2.1 General Rule

Patents are available throughout the world, and are issued on a country-by-country basis. Patents are obtained in the U.S. by filing a patent application with the federal Patent and Trademark Office ("PTO"), pursuant to the Patent Act of 1952.[557] U.S. utility patents expire 20 years after a patent application is filed.[558] Patent protection begins when the patent issues, so the utility patent's life lasts 20 years less the time that the application is pending. Patents filed before June 6, 1995 expire the later of 17 years from the date of issuance, or 20 years from the date of filing.

7.2.2 Applicability to CAs

Patents can protect any "process, machine, article of manufacture, or composition of matter."[559] The Supreme Court has interpreted this very broadly, remarking that patent protection is available for "anything under the sun that is made by man."[560] Accordingly, many of the technologies used by a CA are patented by third parties. For example, the basic idea of public key encryption was patented in 1980, and the specific encryption system that the CA plans to use was patented in 1983.[561] Rights to these patents are held by Public Key Partners of Sunnyvale, California, an affiliate of RSA Data Security, Inc. ("RSDI"). The patents are widely licensed to major developers of CA software and services. Patents could also cover other technologies used by a CA, including security procedures and methods for maintaining repositories and CRLs. For example, a patent issued in 1991 and entitled "Electronic Notary" may cover digital date-time stamping.[562]

---

[557] 35 U.S.C. § 1 *et seq*.

[558] 35 U.S.C. § 154(a)(2); other types of patents have different terms.

[559] 35 U.S.C. § 101.

[560] *Diamond v. Chakrabarty*, 447 U.S. 303, 309 (1980).

[561] U.S. Patent Nos. 4,200,770, 4,218,582 and 4,405,829.

[562] U.S. Pat. No. 5,022,080.

7.2.3 Direct Infringement

A U.S. patent entitles its owner to exclude others from making, using, selling, offering for sale or importing the patented invention.[563] Patent infringement occurs when someone performs one of these acts without the patent owner's permission. The legal definition of the patented invention is specified in the patent's *claims*, which are found at the back of the patent.

There are two types of patent infringement, literal infringement and infringement under the doctrine of equivalents. A patent is *literally* infringed by the unauthorized use, manufacture or sale of a device or process (the *accused device*) that falls within the literal scope of any of the patent's claims. A patent may also be infringed under the *doctrine of equivalents* if the accused device or process includes every claim element or its equivalent, and it performs the same function as the claimed invention in the same manner to achieve the same result.[564] The doctrine of equivalents is a judicial extension of literal infringement. Its purpose is to provide the patentee with a remedy where a defendant has appropriated the essence of the invention, but in some minor way has avoided the technical, literal limitations of the patent claim.[565]

7.2.4 Indirect Infringement

When the CA provides a product or service to its customers, and the use of the product or service by the customers infringes a patent, then the CA's customer is the *direct* infringer of the patent. However, the CA may still be liable as an *indirect* infringer for inducing or contributing to that infringement.[566]

Inducement cases typically involve patents that are infringed by end users at the encouragement or suggestion of a vendor. For example, suppose a vendor sells an instruction manual that explains how users can modify the vendor's software so that it infringes a patent. Under these circumstances, the end users may be the direct infringers, but the vendor is probably liable for inducing infringement.

Contributory infringement cases arise where (1) a defendant sells or imports a component of a patented machine constituting a material part of the invention (2) despite knowing the component to be especially made or adapted for use in infringing the patent, and where (3) the component is not a staple article or commodity of commerce suitable for substantial noninfringing use.[567] For example, suppose a patent claims a method of encryption that is only directly infringed by end users of digital certificates. A vendor who provides digital certificates

---

[563] 35 U.S.C. § 271.

[564] *See Graver Tank & Manufacturing Co. v. Linde Air Products Co.*, 339 U.S. 605, 85 U.S.P.Q. 328 (1950); *Pennwalt Corp. v. Durand-Wayland, Inc.*, 833 F.2d 931, 4 U.S.P.Q.2d 1737 (Fed. Cir. 1987).

[565] For example, if a claim to a machine recited "screws" and the defendant's machine used "bolts," the defendant's machine would not literally infringe. However, a court could, depending on the circumstances, find infringement under the doctrine of equivalents.

[566] 35 U.S.C. §§ 271(b) and 271(c).

[567] 35 U.S.C. § 271(c).

could be liable for the end users' infringement, unless the certificates have substantial noninfringing uses.

7.2.5 Infringement Outside of the U.S.

As a general rule, a U.S. patent is only enforceable within the United States, its territories and possessions.[568] Use of the patented invention in Canada, for example, does not infringe a U.S. patent. To protect the invention in Canada, or other foreign countries, the patentee must procure patents in each separate country. However, a U.S. patent can in some cases be infringed by a party that induces or contributes to the direct infringement of others, even if this direct infringement takes place outside the United States.[569] Liability may apply in these cases if the defendant:

(a) supplies components of a patented invention from the U.S.;

(b) the components are combined outside the U.S. in manner that would infringe the patent if such combination occurred within the U.S.; and

(c) the defendant actively induces or knowingly contributes to the combination.[570]

For example, suppose the CA distributes software to persons outside the United States. The software, when loaded onto a computer, causes the computer to fall within the scope of a machine claim of an issued U.S. patent. Under these facts, the CA could be potentially liable for contributory infringement of the U.S. patent, even though its subscribers are in foreign countries, unless the software has substantial noninfringing uses.

7.2.6 Remedies for Patent Infringement

When a patent is infringed, the patent owner can recover money damages and attorney fees, and can obtain a court order (or "injunction") prohibiting further infringement.[571] Damages for patent infringement can include the profits that the patentee has lost as a result of the infringement. With computer-related inventions, these damages can be significant because lost profits are calculated by deducting only the variable costs from gross receipts.[572] Of course, the real cost of software and computer services is the sunk development and other capital costs. The

---

[568] 35 U.S.C. § 271; *but see also* 35 U.S.C. § 105 ("any invention made, used or sold in outer space on a space object or component thereof under the jurisdiction or control of the United States shall be considered to be made, used or sold within the United States for the purposes of this tile. . . .").

[569] 35 U.S.C. § 271.

[570] Specifically, under 35 U.S.C. 271(f), this requires either that: (i) the defendant supplies at least a substantial portion of the components of the invention and actively induces the combination; or (ii) the defendant supplies a component that is especially made or adapted for use in the invention and not a staple article of commerce suitable for substantial noninfringing use.

[571] 35 U.S.C. § 283.

[572] *Paper Converting Mach. Co. v. Magna-Graphics Corp.*, 745 F.2d 11, 223 U.S.P.Q. 591 (Fed. Cir. 1984).

variable costs of providing computer services or a copy of software (especially with online distribution) are usually low. Thus, in the online industry, lost profit awards may approach the full price of the software or service. If the patentee cannot establish that it is entitled to lost profits, then it at least recovers a reasonable royalty for the infringing activity.[573] In appropriate cases, these money damages can be multiplied up to three times.[574] Also, in "exceptional cases" the patentee can recover its attorney fees.[575]

While money damages in patent cases can be significant, the injunction can be particularly devastating because it can wipe out investments made to produce or market a product. In one dramatic case, Kodak was forced to close its entire instant photography business after it lost a patent infringement suit to Polaroid.[576]

7.2.7 Patents and the CA's Suppliers

Much of the equipment, services and software required for the CA to perform its CA functions will actually be provided by a CMA or other suppliers. For these reasons, we explore in this section the interplay between patent rights and the supplier-customer relationship.

Under the first sale doctrine, when the CA purchases patented equipment from a patentee, it automatically has the implied right to use, repair and resell the patented product.[577] This is also true when the equipment is purchased from a licensee who is authorized by the patentee to make and sell the equipment.

Because software is often licensed rather than sold, the first sale doctrine does not always apply to software-related transactions. Thus, the CA should carefully consider on a case-by-case basis the scope of its express and implied license rights when acquiring patented software or software-related services from a vendor. Also, where its supplier is a mere licensee, the CA should conduct due diligence to confirm that the supplier in fact has the license rights that it purports to have. This can be accomplished by examining the supplier's license, obtaining an estoppel letter from the patentee and/or obtaining the seller's warranty of authority.

The CA would typically look to its supplier to ensure that the supplier's products and services do not infringe third-party patents. If third-party patents are infringed, then it would be customary and appropriate for the supplier to indemnify the CA. This indemnity should not be limited to existing patents, but should also include patents issued on a going-forward basis. The CA should be mindful that a supplier indemnity is only as good as the supplier's financial ability to honor it.

---

[573] 35 U.S.C. § 284.

[574] 35 U.S.C. § 284; generally, enhanced damages are awarded only in cases of willful infringement.

[575] 35 U.S.C. § 285; exceptional cases include cases of willful infringement and cases involving inequitable conduct by the patentee in obtaining the patent.

[576] Forbes ASAP, March 27, 1993, Page 58.

[577] See, e.g., Keeler v. Standard Folding-Bed Co., 157 U.S. 659 (1895) (purchaser can resell and use patented product free of patent monopoly).

When a business relies heavily on outsource service providers, as the CA intends to do, it is tempting to ignore third-party patent infringement on the premise that such issues are the vendor's responsibility. However, it is possible for the CA to infringe a patent by combining or modifying non-infringing subject matter purchased from a vendor. In that situation, it is the CA and not the vendor that is directly liable for patent infringement.

7.2.8 Avoiding Patent Infringement

Unlike copyright infringement, discussed below, patent infringement does not require that the defendant's accused material have been *copied* from the plaintiff's. That is, a defendant can be liable for patent infringement even though it conceived of the patented idea independently and without reference to the original patented invention. Moreover, because pending patent applications are not publicly available and may languish in the PTO for years, a defendant may be surprised to discover that a newly-issued patent covers technology already used by the defendant and long thought to be in the public domain. For these reasons, patent infringement may be hard to detect and avoid.

Although often impractical or cost-prohibitive, the best method for reducing the probability of committing patent infringement is to conduct a comprehensive patent infringement study. This study involves first conducting a search of patents that may be potentially infringed by a proposed activity and then analyzing each patent to determine whether there are serious infringement issues. The cost of this type of study ranges from $50,000 on up, depending on the scope of the search.

7.3 Copyright

7.3.1 General Rule

Copyright protects original works of authorship fixed in a tangible medium of expression.[578] Copyrightable subject matter includes texts, photographs, drawings and computer codes. Under U.S. law, the owner of copyrighted material has the exclusive right to copy, distribute, modify, publicly perform and publicly display the material.[579] Copyright rights are distinct from property rights in that they address physical copies of copyrightable material. For example, if an individual purchases an authorized copy of a book, the individual (not the book's publisher) owns the copy. However, ownership of the copy does not bestow upon the individual any right to copy or modify the book, for example. These rights are retained by the publisher. An important exception to this rule is that the publisher's exclusive right of distribution is extinguished on the first sale of the copyrighted material. Thus, the individual who purchased the book may freely lend or resell it.

[578] 17 U.S.C. § 102(a).

[579] 17 U.S.C. § 106.

7.3.2 Applicability to CAs

The CA deals with copyrightable works in many ways. The software and documentation used to effectuate the CA services is subject to copyright, as may be the repository, CRL and other datCAses, and potentially the format and content of a certificate. Use of these materials in an online environment is especially prone to raise copyright infringement issues because the online transmission of copyrighted material necessarily involves copying and in some cases distribution, public display and public performance of the material. For example, when a datCAse is accessed online, a copy may be made on the user's remote computer.

7.3.3 Infringement

Copyright infringement involves the unauthorized copying, modification, distribution, performance or display of copyrighted works. Unlike patent law, copyrights do not cover independently created works. For example, it is not copyright infringement for a defendant to *independently* develop a certificate datCAse that is identical to a competitor's. However, the law presumes copying when the defendant's work is substantially similar to the plaintiff's and the defendant has had access to the plaintiff's work.[580]

7.3.4 Remedies

A copyright owner is entitled to recover actual or statutory damages. Actual damages are damages suffered by the copyright owner as a result of the infringement and any profits of the infringer that are attributable to the infringement and are not taken into account in computing the actual damages.[581] A court may also award costs and attorney fees to the prevailing party in a copyright lawsuit and grant temporary and final injunctions to restrain further infringement.[582]

7.3.5 Exceptions

The CA may copy, distribute or adapt materials for which it does not own the copyright if:

(a) the content is in the public domain. This applies if the copyright has expired[583] or if the owner has CAndoned the copyright or

---

[580] *See Arica Inst., Inc. v. Palmer*, 970 F.2d 1067, 1072 (2d. Cir. 1992).

[581] 17 U.S.C. § 504(b).

[582] 17 U.S.C. § 505 (as to costs and attorney fees); 17 U.S.C. §502 (as to injunctions).

[583] For works created on or after January 1, 1978, the copyright lasts for the life of the author plus 50 years. The copyright in works for hire expires 75 years after the year of first publication or 100 years after the year of creation, whichever comes first. 17 U.S.C. § 302. Thus, no work created after January 1, 1978 can enter the public domain until 2029 at the earliest. The rules for works created before January 1, 1978 are more complex, and depend on whether the copyright was registered and whether proper notice was used. 17 U.S.C. § 304.

dedicated it to the public domain, or if the work was created by the federal government;[584]

(b) the use is considered *de minimis* or a fair use;[585]

(c) what is copied is not itself copyrightable, such as facts, ideas, or non-original elements;[586] or

(d) the CA obtains permission or a license from the copyright owner that covers the use in question.

7.3.6 Copyrights and the CA's Suppliers

The issues surrounding copyrights and suppliers are comparable to those described in Section 7.2.7 above in connection with patents. However, the following points merit amplification. As with patent law, there is a first sale doctrine for copyrights, under which the sale of copyrighted material by the copyright owner extinguishes the exclusive right of distribution and allows the purchaser to resell the copyrighted material. Section 117 of the copyright statute also provides purchasers of computer software with the right to copy the software to the extent that such copying is an "essential step in the utilization" of the software or is for backup purposes only.[587] In other words, if a customer buys a program, it is entitled by law to install and use it on a single computer, even though the installation and use necessarily involves limited copying (*i.e.*, copying onto the disk drive; copying into the computer's RAM).

The first sale doctrine and the rights under Section 117 only apply to sales transactions. Most software and data is licensed not sold. When software is licensed, the first sale doctrine and Section 117 do not apply and therefore the supplier-licensor can control the licensee's use, installation and disposition of the software.

A CA can reduce the chances of a copyright dispute by: (a) independently creating the software, data or other copyrightable material used in the CA's business; (b) acquiring outright the copyrights to any third party material used in the CA's business; and/or (c) expressly

---

[584] Works created by the U.S. federal government and its employees, such as statutes, speeches, legal decisions, and other government documents, are in the public domain. 17 U.S.C. § 105. This rule applies only to works of the federal government, however, and not to those of state governments. Also, it only applies to works *created by* the federal government, not to works that the government may acquire from others.

[585] Fair use analysis is complex and fact-specific, and there are no hard and fast rules. The courts take into account the following four factors: (1) the *purpose and character* of the use -- is it for commercial or nonprofit purposes? (2) the *nature* of the work copied -- is it factual or creative? (3) the *amount and substantiality* of the copying, as compared to the work as a whole, and (4) the *effect of the use on the potential market* for the work. 17 U.S.C. § 107. If the CA intends to rely on fair use to justify copying materials of third parties, more intensive analysis should be performed based on the specific facts.

[586] Copyright protects the expression of ideas, but does not protect ideas themselves. Section 102(b) of the Copyright Act states that "[i]n no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work. 17 U.S.C. 102(b).

[587] 17 U.S.C. 117.

licensing from the appropriate party the rights to use third-party material used in the CA's business.

As discussed above in connection with patents, the CA should seek contractual indemnification from its suppliers with regard to third-party copyright claims.

7.4 Trade Secrets

7.4.1 General Rule

Under the Uniform Trade Secrets Act ("UTSA"), as adopted in Illinois for example, a trade secret is defined as "information, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or list of actual or potential customers or suppliers, that: (a) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality."[588] Other types of confidential information not meeting that statutory definition of a trade secret may also be protected by contract. For example, two trading partners could agree to hold certain information confidential regardless of whether that information was technically protected under the UTSA.

7.4.2 Applicability to CAs

CAs may encounter other parties' trade secrets in at least two ways. First, the CA may be exposed to trade secrets of a service provider in the CA's role as a customer or licensee. For example, it is conceivable that a CMA may provide trade secret or other confidential information to the CA concerning the CMA's security practices. Second, the CA's customers may provide the CA with secret information in their certificate requests. In either case, the CA may have obligations under contact or statute to preserve the confidentiality of the secret information. Anytime the CA is entrusted with trade secret or other confidential information of another party, it has potential liability exposure if the information is misused or not properly secured.

7.4.3 Infringement

The UTSA prohibits misappropriation of trade secrets, which includes "disclosure or use of a trade secret without express or implied consent" by a person who acquired the secret "under circumstances giving rise to a duty to maintain its secrecy." 765 ILCS 1065/2(b) (Illinois). Apart from the statute, contractual obligations of secrecy may be breached in myriad ways, depending on the specific duties imposed in the contract.

7.4.4 Remedies

Under the UTSA, a court may enjoin actual or threatened misappropriation of a trade secret.[589] If the court determines that it is unreasonable to prohibit future use, it may require

[588] *See* 765 ILCS 1065/2(d) (Illinois).

[589] Uniform Trade Secrets Act, § 2.

payment of a reasonable royalty as a condition for such use.[590] A plaintiff may also recover damages for the actual loss caused by the misappropriation as well as unjust enrichment not taken into account in computing damages for actual loss. If misappropriation is willful, the award of damages may be doubled.[591]

7.4.5 Exceptions

Generally speaking, once a trade secret or other item of confidential information is disclosed to another party without restriction, the proprietary nature of the information is destroyed. Thus, if a supplier were to unilaterally divulge a trade secret to the CA without restriction, that information, as a general proposition, would no longer be protected by trade secret law. However, a disclosing party could, prior to the disclosure, insist that CA agree to maintain the information in confidence, in which case the trade secret status of the information may be preserved.

7.4.6 Economic Espionage Act of 1996

The Economic Espionage Act of 1996 ("EEA") was enacted in response to a perception that economic espionage was threatening U.S. industry.[592] Although the EEA was primarily intended to cover professional espionage sponsored by foreign governments and companies, many commentators have observed that its broad language could criminalize even garden-variety misappropriation of trade secrets.

Under the EEA, almost any financial, business, scientific, technical, economic or engineering information can be protected if the owner has taken reasonable measures to keep the information secret; the information is not in the public domain; and the information derives independent economic value, actual or potential, from not being in the public domain.[593] A person may violate the EEA if, among other things, he or she "copies, duplicates, sketches, draws, photographs, *downloads, uploads*, alters, destroys, photocopies, *replicates, transmits*, delivers, sends, mails, communicates or conveys" the trade secret without authorization of the trade secret owner.[594] A violator must also intend to appropriate the trade secret for the economic benefit of some person other than the owner.

The penalties for violating the EEA are severe. Individuals face 15 years in prison.[595] Organizations can be fined up to $10,000,000.[596] In addition, a party violating the law may be required to forfeit to the United States Government all property constituting or derived from the

---

[590] *Id.*

[591] Uniform Trade Secrets Act, § 3.

[592] 18 U.S.C. §§ 1831-39.

[593] 18 U.S.C. § 1839(3).

[594] 18 U.S.C. § 1832(a)(2) (emphasis added).

[595] 18 U.S.C. § 832(a).

[596] 18 U.S.C. § 1832(b).

proceeds of the theft as well as all property used to commit or facilitate the theft.[597] Conceivably, this forfeiture clause could be interpreted very broadly with catastrophic results for an organization found guilty of a violation.

It is not completely clear how broadly the EEA will be interpreted or enforced. However, in view of the harsh penalties that may be imposed under the EEA, the CA should be particularly careful handling trade secrets and other confidential information of others.

7.5 Trademarks and Unfair Competition

7.5.1 General Rule

Trademarks are words, symbols or other devices used to distinguish the goods or services of one person from those of another.[598] Examples include "Ford" for automobiles and "IBM" for computers. Marks that are used in connection with services are called "service marks." Examples include "American Airlines" for air transportation, "K-Mart" for retail services and "Verisign" for CA services.[599] The owner of a trademark has the exclusive right to use the mark in a particular market on particular kinds of goods or services. Because only one party has the right to use a particular mark in a particular market, trademarks provide consumers with a reliable indication of source. If an unauthorized party uses the same or similar mark in a manner that is likely to confuse consumers, it is liable for trademark infringement and/or the tort of unfair competition.

7.5.2 Applicability to CAs

Trademark law impacts a CA in at least two ways. First, a CA will typically use a trademark or service mark in offering its CA services (*i.e.*, "CA brand certificates"). As in any business, the use of a trademark by a CA raises liability issues if the use infringes a prior user's rights. Second, certificates issued by a CA may contain references to third-party trademarks, particularly in the organization name field of the subscriber's distinguished name. For example, an CA certificate might be issued to the organization "First National Bank." Issuance and use of this certificate may raise trademark and unfair competition issues with respect to the owner or owners of the mark "First National Bank."

7.5.3 Trademark Infringement

Trademarks are protected at both federal and state level. Under the federal trademark law, known as the Lanham Act and codified at 15 U.S.C. 1051 *et seq*., a trademark owner has the exclusive right to use the trademark in a given market, in connection with a particular kind of goods or services. Under Section 32 of the Lanham Act, violation of this right is established by showing that the accused infringer is using a mark that (a) is the same as or similar to the first

---

[597] 18 U.S.C. § 1834.

[598] Trademarks are governed by state law, as well as by a federal statute known as the Lanham Act, 15 U.S.C. § 1051 *et seq*.

[599] The term "trademark" will be used herein to refer to both trademarks and service marks, unless the context otherwise requires.

user's trademark (b) in connection with the sale or advertising of goods or services, and (c) the use is likely to cause confusion as to the source, origin, sponsorship or approval of goods or services.[600]

Likelihood of confusion analysis can be complex and fact-intensive. Courts weigh a number of different factors, including a comparison of the mark's appearance, sound, and connotation,[601] a comparison of the goods and services,[602] the sophistication of relevant consumers,[603] the length of time the marks have co-existed without actual confusion, the relative "strength" of the marks, the prices of the goods and services, and the defendant's good faith in adopting its mark.[604] To avoid disputes with prior users it is advisable to conduct a trademark search before adopting a new mark or extending an existing mark to a new product or service.

Although we have not conducted a trademark search, we note that if the American Bankers Association uses the "CA" designation for its CA services, there may be potential for confusion with the American Bar Association (also known as the CA). The American Bar Association is not offering CA services, but it does have a well-recognized presence in the area of digital signatures, including the publication of guidelines for digital signature legislation.

A definitive analysis of the likelihood of confusion with the American Bar Association requires more specific information, including the specific format of the mark to be used, the manner of presentation, and the intended audience. However, as a preliminary matter, there would appear to be a potential for confusion in this case. Solutions might include modifying the mark to make sure the full association name is prominently used, disclaiming any association with the American Bar Association, and even obtaining the consent of the American Bar Association. Another consideration may be the level of sophistication of the relevant consumers - if all consumers of CA services will be extremely sophisticated and knowledgeable, there is less likelihood of confusion.[605]

Claims for trademark infringement under Section 32 might also provide a remedy against the CA for a party whose trademark or identity has been impersonated or appropriated by an impostor who acquires an erroneously issued CA certificate. The key issue in determining whether a claim under Section 32 would fall under these circumstances is whether the issuance of a certificate amounted to "use" by the CA of the infringed mark "in commerce." This point is considered in Section 7.5.6 below.

---

[600] 15 U.S.C. § 1114(1)(a).

[601] *Franklin Mint Corp. v. Master Mfg.*, 667 F.2d 1005 (C.C.P.A. 1981).

[602] *Merriam-Webster, Inc. v. Random House, Inc.*, 35 F.3d 65 (2d Cir. 1994).

[603] *Bristol-Meyers Squibb v. McNeil-P.P.C.*, 973 F.2d 1033 (2d Cir. 1992).

[604] *Polaroid Corp. v. Polaroid Electronics Corp.*, 287 F.2d 492 (2d Cir. 1961).

[605] Note that the relevant consumers will fall into a number of groups. The subscribers, being banks, will of course be sophisticated and not likely to be confused. The relying parties, however, may be less sophisticated, depending on how the certificates are to be used.

7.5.4 Unfair Competition

Trademark infringement is but a single species of a broader class of torts known as unfair competition, which among other things, generally prohibits false designations and false descriptions. Unfair competition is addressed in Section 43(a) of the Lanham Act, which provides liability for any person who:

> (a) on or in connection with any goods or services
>
> (b) uses in commerce
>
> (c) any word, term, name, symbol, or device
>
> (d) which is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person.[606]

This provision may allow a remedy against the CA for a party whose trademark or identity has been impersonated by an impostor who acquires an erroneously issued CA certificate. For example, suppose that the CA issues a certificate to an impostor posing as an authorized representative of the First National Bank. Such a certificate will include the impostor's public key and the trade name or trademark of the First National Bank. Arguably, under these facts, the First National Bank may have a claim against the CA under Section 43 because the CA appears to be (a) using in commerce (b) the name "First National Bank" (c) in connection with goods or services (*i.e.*, the certificate) (d) in a manner that is likely to cause mistake as to the connection or approval of the certificate by the First National Bank. Whether a claim exists here under Section 43(a) depends on whether issuance of the certificate meets the "use in common" requirement. This is discussed in Section 7.5.6 below.

7.5.5 Dilution

Under Section 43(c) of the Lanham Act, the owner of a "famous mark" is entitled, subject to the principles of equity, to an injunction against another person's commercial use of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark.[607] This "anti-dilution" provision is specifically designed to protect famous marks in situations where the defendant's use of the mark does not cause confusion but might blur, tarnish or disparage the famous mark.[608] Courts have found, for example, that use of a famous mark as a domain name constitutes dilution under the Lanham Act.[609]

---

[606] 15 U.S.C. § 1125(a).

[607] 15 U.S.C. § 1125(c).

[608] *See, e.g., Intermatic Inc. v. Toeppen*, 947 F. Supp. 1227, 1238 (N.D. Ill. 1996).

[609] *Id*. at 1239.

Although there are no cases on record, one could argue that Section 43(c) would provide the owner of a famous trademark with injunctive relief against the CA if the CA were to issue erroneously a certificate to an impostor under the famous trademark (*e.g.*, CACA issues a certificate listing "Chevrolet" as the subscriber to a person who was not related to Chevrolet).

7.5.6 Use in Commerce Requirement

We have articulated in the preceding three sections potential claims against the CA that could conceivably be lodged by a party whose mark has been used by an impostor in an erroneously-issued CA certificate. In each of these potential claims, the would-be plaintiff has the burden of establishing that the CA's activity (*i.e.*, the erroneous issuance of a certificate) constituted a "use in commerce" of the plaintiff's mark (or, in the case of dilution under Section 43(c), "commercial use" of the plaintiff's mark).

The Lanham Act defines "use in commerce on goods" as occurring when the mark "is placed in any manner on the goods or their containers or the displays associated therewith or on the tags or labels affixed thereto, or if the nature of the goods makes such placement impracticable, then on documents associated with the goods or their sale."[610] The act defines "use in commerce on services" as occurring when the mark "is used or displayed in the sale or advertising of services and their services are rendered in commerce ..."[611]

Under these definitions, it is not clear that erroneous issuance of a certificate constitutes "use in commerce *on* goods" or "use in commerce *on* services." While this potentially supports the argument that the CA is not using the infringed marks in commerce, the provisions of the act discussed above [Sections 32, 43(a) and 43(b)] are not predicated solely upon a use in commerce *on* goods or *on* services. Section 32 speaks of "use in commerce ... of a registered mark *in connection with* the sale, offering for sale, distribution or advertising of any goods or services." Section 43(a) speaks of use "*on or in connection with* any goods or services." Section 43(c) speaks to "commercial use" in commerce of a mark (without reference to goods or services). This variance in terminology arguably means that the narrow specifications in the definition of use in commerce "on goods" and "on services" are not intended to limit causes of actions under Section 32, 43(a) and 43(c). In fact, Congress specifically amended Section 43(a) to include the "in connection with" language, and this amendment has been construed by at least one court as dispensing with the requirement that a defendant cause goods or services to enter commerce.[612]

Thus, the statutory definitions of "use in commerce" do not seem to resolve the issue. Some additional guidance on this point is provided by litigation involving the domain-name registrar Network Solutions, Inc. (NSI).[613] NSI is a registrar that assigns domain names such as "CA.com" to users. A domain name is an alphanumeric symbol for a numeric Internet address.

---

[610] 15 U.S.C. § 1127 ("use in commerce").

[611] *Id.*

[612] *Juno Online Services, L.P. v. Juno Lighting, Inc.*, 979 F. Supp. 684 (N.D. Ill. 1997).

[613] *Lockheed Martin Corporation v. Network Solutions, Inc.*, ___ F. Supp. ___, 44 U.S.P.Q.2d 1865 (C.D. Cal. 1997); *Academy of Motion Picture Arts and Sciences v. Network Solutions, Inc.*, ___ F. Supp. ___ (1997 WL 810472) (C.D. Cal. Dec. 22, 1997).

Numeric addresses tend to be unintelligible to humans (*e.g.*, 00.33.121.38), while domain names are often easy-to-remember mnemonics (*e.g.*, "flowers.com"). With a domain name, users are spared the cumbersome task of entering the numeric address. Domain names can also have significant trademark implications when famous marks are used as domain names (*e.g.*, "microsoft.com").

In maintaining its registry, Network Solutions promulgates a datCAse of users and their corresponding domain names and numeric addresses. Some unscrupulous individuals have "hijacked" domain names consisting of famous trademarks such as "mcdonalds.com" and "academyaward.com." These individuals frequently seek to profit by selling the hijacked domain name to the owner of the corresponding trademark. Typically, the trademark owner sues the hijacker directly for various Lanham Act violations.

In two recent cases, however, the trademark owners sued Network Solutions, asserting that the conduct of Network Solutions in registering the domain names violated the Lanham Act. In both cases, the courts held that Network Solutions had not "used the mark" in commerce, and consequently, had not violated the Lanham Act.

The first case, *Lockheed Martin Corporation v. Network Solutions, Inc.*, involved a claim by Lockheed against NSI for registering domain names that were identical or similar to Lockheed's "Skunk Works" service mark. In granting NSI's motion for summary judgment, the court held that NSI did not "use in commerce" Lockheed's marks in the manner required to establish a Lanham Act violation. In particular, the court found that NSI "merely used domain names to designate host computers on the Internet." According to the court, this function was "purely nominative" and "pure machine-linking" and was not the type of trademark use giving rise to infringement. The court contrasted the role of NSI to that of a telephone directory publisher who violates the Lanham Act by printing an infringing trademark in the yellow pages. In that case, the court reasoned, the publisher has "supplied the material that directly caused the likelihood of confusion." NSI, in contrast, does not provide "the instrument or forum for infringement."[614] The court found this rationale applicable to Lockheed's claims under Sections 43(a) and 43(c).

The second case, *Academy of Motion Picture Arts and Sciences v. Network Solutions, Inc.*, reached the same result on similar reasoning. The plaintiff in *Academy* sought a preliminary injunction against NSI for registration of domain names that included variations of the plaintiff's famous "Academy Awards" mark. Relying on the above-cited definitions of "use in commerce" and citing *Lockheed*, the court denied the Academy's motion for injunctive relief.

Lockheed and *Academy* are comforting precedents because a CA's role as a registrar in some respect is analogous to that of NSI. However, a CA differs from NSI in at least two critical respects. First, unlike NSI, a CA arguably does provide the "instrument and forum" for the infringement by supplying a certificate binding a public key to a trademarked term such as "Citibank." The court in *Lockheed* relied on this point to distinguish NSI from director publishers who had been found to violate the Lanham Act. It is not clear that this rationale would apply in the case of a CA, which undertakes an identity verifying and binding function.

---

[614] *Lockheed*, *supra*, at 8-9.

Second, the certificates that the CA proposes to issue will be supplied to banks which will in turn use those certificates to offer CA and banking services to others. If one considered the banks as purveyors of goods and services (*i.e.*, certificates and financial services), then the CA-supplied certificate arguably functions as a label that is used in connection with those goods and services. Application of a trademark to a label falls within the statutory definitions of "use in commerce." Thus, label providers such as printers can violate the Lanham Act by creating infringing labels at the request of their customers, even if the printers do not know the labels are infringing.[615]

7.5.7 Infringer Innocent Defense

The Lanham Act does not require the plaintiff to establish intent on the part of the defendant, and claims under the Lanham Act can ensnare printers, publishers and others who innocently reproduce an infringing trademark at the request of a customer.[616]

To ameliorate this strict liability, the statute provides special relief for certain innocent infringers when either:

- (a) the infringer or violator is engaged solely in the business of printing the mark or violating matter for others and establishes that he or she was an innocent infringer; or
- the alleged infringement or violation is contained in or is part of paid advertising matter in a newspaper, magazine, or other similar periodical or in an "electronic communication."[617]

If applicable, this "innocent infringer" defense would shield a CA from monetary damages for violations under the Lanham Act.[618] However, there are at least two hurdles a CA must leap before the defense would be applicable. First, the CA would have to persuade the court that its activities fell within the first exception ("engaged solely in the business of printing the mark"). The sparse case law on this provision does not offer much guidance as to whether the term "printing" could be construed broadly enough to encompass a CA business. This issue requires further study.

Second, even assuming that a CA is a "printer" (and therefore entitled to assert the defense), the CA must also demonstrate that it was an "innocent infringer." Courts have held that to be an innocent infringer, a printer must make objectively reasonable efforts to determine if its customer is authorized to use the mark in question. For example, *Polo Fashions, Inc. v. Ontario Printers* was a Lanham Act suit over counterfeit Polo brand clothing. The defendants included a corporate printer and an individual, one Lasky, whose relationship to the printer is not clearly specified. Although the opinion does not detail the operative facts, it appears that the

---

[615] See, e.g., *Conopco, Inc. v. Rosa Distributors*, 967 F. Supp. 1068 (N.D. Ill. 1997); *Polo Fashions, Inc. v. Ontario Printers, Inc.*, 601 F. Supp. 402 (N.D. Ohio, 1984).

[616] *See, e.g., Burger King Corp. v. Majeed*, 805 F. Supp. 994 (S.D. Fla. 1992).

[617] 15 U.S.C. § 1114(2).

[618] *Id.*

defendants unwittingly printed infringing materials for a customer who was trafficking in counterfeit Polo merchandise.[619] In granting Polo's motion for a preliminary injunction and partial summary judgment, the court admonished that business persons "cannot be naive and be like ostriches and put their head in the sand and ignore obvious facts that should be apparent to a reasonable business person."[620] In particular, the court held:

> When a person, such as a manufacturer or a printer, is approached to make a product for a famous manufacturer, that business person *has an affirmative duty to determine the legitimacy of the person placing the order.* That person must make reasonable inquiry, and this will be determined from all of the facts and circumstances.[621]

A more recent decision, *Conopco, Inc. v. Rosa Distributors*, has cited and followed *Polo Fashions.*[622] In *Conopco,* the defendant, a printer, received an order to print labels for "Nuggles" fabric softener. The labels were subsequently found to infringe the mark "Snuggles" for fabric softener. The trademark owner sued the printer for trademark infringement in the Northern District of Illinois. In denying the defendant's motion for summary judgment, the court held that the innocent infringer defense was not available. Citing *Polo Fashions,* the court in *Conopco* held that while a printer is not required in every case to investigate a customer's authorization to print product labels, its conduct must be objectively reasonable.[623]

7.5.8 Remedies

Under the Lanham Act, a successful plaintiff is entitled to the defendant's profits, and "any damages" sustained by the plaintiff and costs of the action.[624] The court may treble these damages and, in exceptional cases, may award reasonable attorney fees. Plaintiffs may also be entitled to injunctions against further infringement.[625]

7.5.9 Lanham Act Summary

Like any business that adopts a new mark, the CA should conduct a clearance study to ensure that its CA brand as applied to CA services will not infringe a prior user's rights. We have identified the American Bar Association as one prior user who may conceivably object to use of "CA" on CA services. CAs may also be liable to trademark owners under the Lanham Act for issuing to unauthorized persons certificates that list their trademarks. However, the issue

---

[619] *Polo Fashions, Inc. v. Ontario Printers, Inc.*, 601 F. Supp. 402 (N.D. Ohio, 1984).

[620] *Id.* at 403.

[621] *Id*. (emphasis supplied).

[622] *Conopco, Inc. v. Rosa Distributors*, 967 F. Supp. 1068 (N.D. Ill. 1997).

[623] *Id*. at 1071.

[624] 15 U.S.C. § 1117(a)(2); *see also McCarthy on Trademarks*, § 30:72 (remarking that plaintiff's damages should be measured by the tort standard under which the infringer-tortfeasor is liable for all injuries caused to plaintiff by the wrongful act, whether or not actually anticipated or contemplated by the defendant).

[625] 17 U.S.C. § 1116.

of liability is not clear-cut, and in any case the CA may have an innocent infringer defense which would limit the remedy against the CA to injunctive relieve. The innocent infringer defense, if applicable, will only be available if the CA has acted in an objectively reasonable manner in determining that the subscriber of the certificate was authorized to use the mark at issue. Overall, this point should be given further study.

7.6 Privacy

Because the CA will be generating certificates (and gathering information) only with respect to banks, and not with respect to individuals, there should be less concern for potential invasion of privacy. However, the following section will briefly outline the relevant law in this area, for general reference.

The common law right of privacy is based on the general principle that each person has the "right to be left alone."[626] In some states, it is also protected by statute. In either case, the rules regarding the right of privacy will vary from state to state.

Essentially, there are three types of right of privacy violations that potentially impact CAs:[627]

- publicity which places a person in a *false light*, in a manner that is highly offensive to a reasonable person;[628]
- *misappropriation* of a person's name or likeness for commercial purposes, such as for an advertisement;[629] and
- *public disclosure* of embarrassing private facts.[630]

The potential for privacy violations in the context of a CA's operations seems remote. However, one could hypothesize an advertisement where the CA shows a picture of a person

---

[626] *Garner v. Triangle Publications, Inc.*, 97 F. Supp. 546, 548 (D. N.Y. 1951); *Diaz v. Oakland Tribune, Inc.*, 188 Cal. Rptr. 762, 139 Cal. App. 3d 118 (1st Dist. 1983).

[627] *See* William L. Prosser, *Privacy* 48 Cal. L. Rev. 383 (1960); Restatement (Second) of Torts, §§ 652A-652I (1977). *See also Haynes v. Alfred A. Knopf, Inc.*, 9 F.3d 1222, 1229 (7th Cir. 1993).

[628] *See*, *e.g.*, *Time, Inc. v. Hill*, 385 U.S. 374, 391-94, 87 S.Ct. 534, 544-45 (1967). These cases often involve placing a person's photograph or image in an embarrassing context. See *Easter Seal Society for Crippled Children & Adults v. Playboy Enterprises, Inc.*, 530 So. 2d 643 (La. Ct. App.), *cert. denied*, 532 So. 2d 1390 (La. 1988) (stock footage of people in a parade used as background in an adult movie); *Parnell v. Booth Newspapers, Inc.*, 572 F. Supp. 909 (W.D. Mich. 1983) (using a photo of an innocent woman for an article on prostitution).

[629] *See*, *e.g.*, *Carson v. Here's Johnny Portable Toilets, Inc.*, 698 F.2d 831 (6th Cir. 1983); *Martin Luther King, Jr. Center For Social Change, Inc. v. American Heritage Products, Inc.*, 296 S.E.2d 866 (2d Cir. 1953), *cert. denied* 346 U.S. 816 (1953); 346 U.S. 816 (1953); *Douglass v. Huster Magazine, Inc.*, 769 F.2d 1128, 1138-39 (7th Cir. 1985).

[630] *See*,. *e.g.*, *Haynes v. Alfred A. Knopf, Inc.*, 8 F. 3d 1222, 1229-35 (7th Cir. 1993); *Daily Times Democrat v. Graham*, 276 Ala. 380, 162 So.2d 474 (Ala. 1964); *Barbara v. Time, Inc.*, 348 Mo. 1199, 159 S.W.2d 291 (Mo. 1942); *Diaz v. Oakland Tribune, Inc.*, 139 Cal. App. 3d 118, 188 Cal. Rptr. 762, 767-78 (1st Dist. 1983); *Banks v. King Features Syndicate, Inc.*, 30 F. Supp. 352 (S.D. N.Y. 1939).

using the CA digital certificate to verify a bank transaction. If the picture were used without permission, there could be a violation of the right of privacy.[631]

There is increasing concern about the treatment of data that is collected about individuals. For example, government agencies collect extensive information about individuals through military records, social security records, Medicare payments, tax payments, and the like. Similarly, private entities such as banks, credit card companies, stores, insurance companies, and credit reporting agencies maintain extensive datCAses of information about individuals.

In the U.S., the collection, communication, and use of this type of information is still largely unregulated. To the extent that individuals have a right of privacy with respect to this information, it is usually provided only by a limited statute that applies to a specific entity (such as the government) or to specific industries (such as the credit reporting industry, etc.).

For example,

- the Privacy Act of 1974 imposes limits on the collection and use of personal information by federal government agencies.[632] Although there are a number of exceptions, the Privacy Act generally prohibits any government agency from disclosing any record relating to an individual without the individual's consent.[633] The Act does not apply to the collection of personal information by private entities.

- The Fair Credit Reporting Act[634] controls the use of consumer credit reports issued by consumer reporting agencies.

- The Equal Credit Opportunity Act[635] prohibits creditors from gathering certain types of information from credit applicants, such as sex, race, color, religion, national origin, birth control practices, or child bearing plans.[636] Thus, an interesting question might be raised if such information is contained in digital certificates which are reviewed by creditors in the course of verifying digital signatures.

- The Federal Right to Financial Privacy Act of 1978[637] limits the ability of financial institutions to disclose customer information to agencies of the federal government.

---

[631] In addition, while not discussed here, there would be a violation of the right of publicity.

[632] Codified in major part at 5 U.S.C. § 552(a).

[633] 5 U.S.C. § 552a(b).

[634] 15 U.S.C. § 1681, *et seq*.

[635] 15 U.S.C. § 1691, *et seq*.

[636] Reg. B, 12 C.F.R. §§ 202.5(d)(iii)-(v).

[637] 12 U.S.C. § 3401, *et seq*.

- Several states have also enacted legislation addressing limited aspects of financial privacy.[638] There are also certain restrictions on disclosure of medical and employment information, which are likely irrelevant to any CA activities.

[638] *See* 1 George Trubow, Editor, *Privacy Law and Practices*, § 3.03(iv)(d) at p.3-82.

8. LIABILITY OF A PARTY FOR THE ACTS OF ANOTHER

This section outlines the following legal theories under which a defendant could be found liable for the torts or crimes of others:

(a) vicarious liability,
(b) agency,
(c) corporate negligence, and
(d) liability for the criminal conduct of a third party.

8.1 Applicability to CA's

Many (and perhaps most) of the injuries that may flow from or relate to the activities of a CA are likely to be caused not by the corporate persona of the CA but rather by the CA's employees, contractors, subscribers and other third parities. Consider these scenarios:

- the CA's own employees conspire to issue erroneous certificates using the CA's signing key as part of a plan to defraud and injure a third party;

- a CA delegates the function of certificate manufacturing to a contractor, whose employees negligently misuse the CA's signing keys, resulting in the issuance of erroneous certificates which then injure a third party;

- a third party malefactor gains access to the CA's signing key, either by physical intrusion or computational attack, allowing the malefactor to create an erroneously issued certificate and thereby perpetrate a fraud to the injury of the purported subscriber and the relying party;

- a malefactor impersonates a fictitious candidate subscriber using forged driver's license and other seemingly authentic identification documents; despite careful and non-negligent adherence to its published policies, the CA issues a certificate to the impostor who uses the erroneously issued certificate to perpetrate a fraud to the injury of a relying party.

In each example, the CA has not committed any wrong-doing that directly caused the injury. However, the question remains as to whether the CA will be held liable for the wrong-doing of others. To help answer this question, this section surveys the above-described legal theories where a party is held liable for the acts of another.

8.2 Vicarious Liability

8.2.1 Generally

Vicarious liability (or *respondeat superior)* is generally defined as the imposition of liability upon one party for the wrong committed by another party.[639] It is grounded on the existence of a relationship whereby one party has the right or ability to control the other. The most common relationships giving rise to vicarious liability are those of master-servant, independent contractors and principal-agent. It is in terms of these relationships that our discussion of vicarious liability is organized.

8.2.2 Master-Servant

A *servant* is a person who is employed to perform services in the affairs of another and whose physical conduct in the performance of the service is subject to the other's control.[640] A servant is distinguished from an *independent contractor* by several factors, including: the extent of the master's control over the details of the work; whether the person employed is engaged in a distinct occupation or business; the skill required in the particular occupation; which party supplies the instrumentalities and place of work for the tasks performed; the method of payment; and the intention of the parties.[641]

As a rule of thumb, employer-employee relationships are master-servant relationships, although there may be exceptions in cases where the employer does not have the requisite degrees of control over the employee.[642] Accordingly, this memorandum uses the terms "employer-employee" interchangeably with "master-servant." Under the law of agency discussed below, a servant-employee is also the agent of his master-employer. An independent contractor (as distinct from a servant) may or may not be an agent depending upon the circumstances.[643]

Once the relationship of master-servant is established, the master becomes vicariously liable for the servant's torts committed within the *scope of the servant's employment*.[644] The rationale for this doctrine are that the master has control over the servant and as against an innocent plaintiff, the master should bear the cost of the servant's wrong-doing because the master is in the best position to absorb and prevent the loss.[645]

---

[639] *See, generally,* A. Skyes, *The Boundaries of Vicarious Liability: An Economic Analysis of the Scope of Employment Rule and Related Legal Doctrines*, 101 Harv. L. Rv. 563 (1988), p. 563.

[640] *See* Restatement (Second) of Agency, § 220(1).

[641] *See* Restatement (Second) of Agency, § 220(2)

[642] *See* Restatement (Second) of Agency, § 2(1)-(2) (1958); Prosser and Keeton on Torts (Fifth Ed.) p. 501-08.

[643] See Restatement (Second) of Agency, § 2(3).

[644] Prosser and Keeton, *supra note 4* at 501-502.

[645] Prosser and Keeton, supra note 4 at 500.

An important limitation to the master's liability is that the tort must take place within the "scope of employment." The Restatement (Second) of Agency defines the "scope of employment" as conduct that: (a) is of the kind the employee is employed to perform; (b) occurs substantially within the authorized time and space limits; (c) is actuated, at least in part, by a purpose to serve the master, and (d) if forcible, is not unexpected by the master.[646]

According to Prosser, the scope of employment encompasses "acts which are so closely connected with what the servant is employed to do, and so fairly and reasonably incidental to it, that they may be regarded as methods, even though quite improper ones, of carrying out the objectives of the employment."[647] Other commentators have said that a tort is within the scope of employment if "it can be said rationally that the employment is the primary cause of the tort."[648]

While the scope of employment may be a broad concept, it is not without boundaries. Torts committed by the employee on his own time that have no bearing on employment will generally not give rise to vicarious liability.[649] Likewise, even during working hours, courts have held that the employer is not liable where the employee's tort is committed while the employee is on a "frolic and detour."[650] More problematic are cases where the employee has committed an intentional tort such as fraud or battery. Early law held that the employer was not vicariously liable for such torts if they were committed for the employee's own purposes but would be liable if the torts where committed to serve the employer (however misguided the employee may have been).[651]

The modern trend, however, is to recognize that such torts may be so reasonably connected with the employment as to be within its scope, thus making the employer vicariously liable. In particular, when the tort is perpetrated to further the interest of the employer, courts are generally willing to impose liability.[652] Even when the employee's purposes are adverse to the employer's interest, liability may be imposed if the employer provided an opportunity for the tort to take place. For example, a federal district court held that a trucking company could be vicariously liable for a rape of a customer committed by its delivery man because the delivery man's "badge of employment" enabled him to gain access to the victim's premises.[653]

---

[646] Restatement (Second) of Agency, § 228(1).

[647] Prosser and Keeton, *supra note 4* at 502.

[648] W. Seavey, Handbook of The Law of Agency 148 (1964).

[649] *Cosgrove v. Lawrence*, 522 A.2d 483 (N.J. Supr. 1987) (therapists sexual involvement with patient outside scope of employment).

[650] *See* Prosser and Keeton, *supra note 4* at 503 and cases cited therein.

[651] *See, e.g.*, Restatement (Second) of Agency, § 228 (1958); Prosser and Keeton, *supra note 4*, at 505-06.

[652] See, e.g., *Rogers v. Kemper Constr. Co.,* 50 Cal. App. 3d 608 (1975).

[653] *Lyon v. Carey*, 533 F.2d 649 (D.C. Cir. 1976).

8.2.3 Independent Contractor

The general rule for independent contractors is that the customer is not vicariously liable for the contractor's torts.[654] The rationale for this general rule is that, because the customer has no right to control the manner in which the work is performed, it is the contractor, not the customer, who is responsible for absorbing and preventing losses.[655] There are at least two exceptions to this rule: non-delegable duties and inherently dangerous activities.[656]

A *non-delegable duty* is a duty from which a party cannot be absolved and with respect to which it may be vicariously liable for the negligence of an independent contractor. Non-delegable duties may arise by statute,[657] contract[658] or common law.[659] For example, the duty of a landlord to maintain common areas and the duty of a railroad to maintain safe crossings have been considered non-delegable.[660]

Prosser reports that it is difficult to suggest any criterion by which the non-delegable character of duties may be determined, other than the conclusion of the court that the responsibility is so important to the community that the defendant should not be permitted to transfer it to another.

Under the Utah Digital Signature Statute, certain duties imposed on the CA may be non-delegable. For example, the statute provides that "[a] certification authority, whether licensed or not, may not conduct its business in a manner that creates an unreasonable risk of loss to subscribers of the certification authority, to persons relying on certificates issued by the certification authority, or to a repository."[661] Arguably, this duty is non-delegable and if so, a CA would be liable for any conduct of its independent contractor that breached this duty.

An inherently dangerous undertaking may also give rise to liability on the part of a customer for acts of its independent contractor. Although the term "inherently dangerous" is not subject to precise definition, it seems to mean activities in which there is a high degree of risk, such as demolition, or keeping dangerous animals.[662] It is not clear that the mere risk of financial loss (such as is attendant in issuing digital certificates) would be considered inherently dangerous.

---

[654] See Restatement (Second) of Agency § 219; Restatement (Second) of Torts § 409; Prosser and Keeton, supra note 4, at 501-16.

[655] Id.

[656] The customer may also be responsible under other legal theories of agency and corporate negligence, discussed below

[657] *Zimmer v. Chemung County Performing Arts*, 482 N.E.2d 898 (1985).

[658] *Kelly v. Howard S. Wright Construction Co.*, 582 P.2d 500 (1978).

[659] See Prosser and Keeton, *supra note 4* at 511, n.26 (and cases cited therein).

[660] Id., n. 29.

[661] Utah Code Ann. 46-3-204.

[662] *See* Prosser and Keeton, *supra note 4* at 512.

8.2.4 Agent

Although a party is generally not liable for the torts of its independent contractors, liability may arise if the contractor is also an agent of the party. Agency is a fiduciary relation in which one person (the agent) acts on behalf of and subject to the control of another person (the principal).[663] While a servant (be he a janitor or an executive) is always an agent, an independent contractor may or may not be an agent depending upon the circumstances.[664]

Agency arises from a manifestation of consent by both the agent and the principal. However, the existence of the relationship does not depend upon the intent of the parties to create it. For example, if a CA proposes to retain a CMA to (a) securely hold the CA's private CA signing key, and (b) use that key to digitally sign CA-denominated certificates at the command of the CA. Arguably, this relationship establishes an agency because the CMA (the putative agent) will be entrusted with the CA's private key (a fiduciary relationship) and will use that private key to digitally sign certificates on behalf of the CA (the putative principal), subject to the CA's control.

The central feature of an agency is the agent's *authority*, which is the power to bind his principal and otherwise alter the legal relations between the principal and third parties.[665] This power is the basis for the liabilities discussed below. The agent's authority may be actual or apparent. Actual authority arises from a consentual relationship between principal and agent, such as the relationship between the a CA and a CMA.[666]

Apparent authority stems from the manifestation by a principal that another is his agent, the manifestation being made to a third person and not to the agent.[667] Arguably, an outsource provider such as CMA has some degree of apparent authority arising from its possession of the CA's private signing key. True, the CA may not have held out the CMA by name to the world. However, the CA has issued a CA certificate binding the CA's identity to the public key that corresponds to CA's private key. By disseminating this certificate, the CA is in effect telling all the world that anyone in possession of the CA's private key is an employee, contractor or other agent who has authority to act on behalf of the CA.

Once an agency is established, the actions of the agent may give rise to liability on the part of the principal. If apparent authority exists, the agent's actions can bind the principal even if they are outside of the scope of the agent's actual authority. The policy underlying this rule is that where one of two innocent parties must suffer from the wrongful act of another, the loss

---

[663] *See* Restatement (Second) of Agency, § 1(1).

[664] As explained above, a servant is automatically the master's agent, although as explained above the liability of a master for the torts of his servant will be greater than the liability of a principal for the torts of an agent who is not a servant. Restatement of Agency, Second, sec. 1, Comment e.

[665] Restatement (Second) of Agency, § 7.

[666] *Id*., Comments b. and c.

[667] Restatement (Second) of Agency, § 8;

should fall upon the one who, by his conduct, created the circumstances that enabled the third party to perpetrate the wrong and cause the loss.[668]

We consider principal's liability in the context of contracts, negligence and intentional torts.

Contract. A principal is responsible for the unauthorized transactions and representations of an agent in connection with a contract if the contract is authorized and if true representations as to the same matter are within the authority or the apparent authority of the agent.[669] The fact that the agent is acting for its own benefit does not relieve the principal of liability unless the relying party has notice that the agent is not acting on the principal's behalf.[670]

Negligence. A principal is generally not liable for physical harm caused by the negligence of a non-servant agent during the performance of the principal's business. There are, however, at least two exceptions: non delegable-duties and misrepresentations.

The non-delegable duty exception states that if the principal was under a duty to have the act performed with care, that duty is non-delegable; therefore, the principal is liable for the physical harm to persons or tangible things caused by the negligence of a non-servant agent. This echoes the non-delegable duty principle discussed above in connection with the vicarious liability of independent contractors. Note that under Utah law, the CA acting as principal has a duty of care imposed by statute that is owed to subscribers, relying parties and repositories. Under the non-delegable duty exception, a CA is liable for the negligence of its agent causing physical harm in violation of this duty.

The misrepresentation exception states that the principal is also liable for physical harm caused by the making of a representation which the agent is authorized or apparently authorized to make or which is within the power of the agent to make for the principal.[671] In this exception we see a crucial difference between agents and mere independent contractors: the agent, who is deemed to act on behalf of the principal, has substantially greater power to render his principal liable to others, particularly in making representations.

Thus, in Section 249 of the Restatement (Second) of Agency it is said that "a master is subject to liability for the misrepresentations of a servant causing pecuniary loss as he is for the misrepresentation for an agent who is not a servant. The comments to Section 249 clarify that the misrepresentation may either be intentional or negligent.

This principle is echoed in § 257 of the Restatement, which says that a principal is subject to liability for loss to another caused by the other's reliance upon on a *tortious*

---

[668] 3 AM. JUR. 2d Agency § 81 (1986).

[669] See, e.g., Restatement (Second) Agency, §§ 161-161A.

[670] See 3 AM. JUR. 2d Agency § 82 (1986).

[671] Restatement (2nd) of Agency, §§ 250-251.

representation of an agent if the representation is authorized, apparently authorized or even within the power of the agent to make for the principal. It is not clear whether "tortious" as used here is limited to intentional torts or would include corporate negligence.

Intentional Torts. Under Section 261 of the Restatement, a principal who puts an agent in a position which enables the agent, while apparently acting within his authority, to commit a fraud upon third persons is subject to liability to such third persons for the fraud.[672] The comments accompanying this provision provide a useful illustration of how this rule could be applied:

> (A) a local manager of (P), a telegraph company, sends a telegram to (T), which purports to come from a person known to (T) asking that (T) send money to him. T sends money addressed to this person through an express company of which A is also a local agent. The telegraph company is subject to liability to T for the amount sent and stolen by (A).[673]

The Restatement specifies that the principal is subject to liability although he is entirely innocent and although the agent acted solely for his own purposes. Liability is based on the fact that the agent's position facilitated the consummation of the fraud and the policy that as between the innocent victim and the principal, the principal is in the best position to bear and prevent the loss.

8.3 Corporate Negligence

The preceding discussion of vicarious liability presented circumstances where a party who has done no wrong may be liable for the torts of a servant, contractor or agent. Liability is imposed as a matter of policy, not fault. Employers and principals may also be liable for negligence in their own right with respect to the way they handle the relationship with the servant, contractor or agent who is primarily at fault. Under this alternate line of reasoning (sometimes called corporate negligence), the employer or principal is said to owe a duty to the injured plaintiff to exercise reasonable care in the hiring, retention or supervision of the person directly responsible for injuring the plaintiff.[674]

8.3.1 Negligent Hiring

Negligent hiring cases typically involve intentional torts by employees with a history of criminal conduct or violent behavior that makes them unfit for the job that they are hired to perform.[675] The employer owes a duty of care to foreseeable plaintiffs to conduct a careful background check on applicants for such positions and to reject those applicants whose backgrounds are unsuitable. The scope of the employer's duty may relate to the position at issue.

---

[672] Restatement (2nd) Agency § 261.

[673] *Id.*, Comment a., Illustration 1.

[674] *See generally,* Hospital Vicarious Liability for the Negligence of Independent Contractors and Staff Physicians: Criticisms of Ostensible Agency Doctrine in Ohio, 56 U. Cin. L. Rev. 771, 713, n. 3 (and cases and materials cited therein).

[675] See Prosser and Keeton, *supra* note 4 at 512.

For example, the duty with respect to security guards may be greater than with respect to a receptionist.[676]

Arguably, personnel charged with performing the critical duties of a CA (such as approving applications for certificates or retaining physical custody of keys) hold the types of positions for which a CA-employer may have a heightened duty of care. This higher duty is codified in the Utah statute, which requires that licensed CAs ensure that their "operative personnel" meet certain specified requirements and have never been convicted of a felony or crime involving fraud, false statement or deception.[677] Utah's definition of "operative personnel" includes contractors and agents, underscoring the non-delegable nature of this duty. Thus, under Utah law, a CA may be liable not only for his own negligent hiring of operative personnel, but also for the negligent hiring of personnel by the CA's contractors.

8.3.2 Negligent Supervision

The duty of reasonable care in supervision stems from similar policy considerations as outlined above in connection with hiring. With respect to employees, the duty even extends to acts outside the scope of employment as necessary to "prevent [the servant] from intentionally harming others or from so conducting himself as to create an unreasonable risk of bodily harm to them."[678] This extended duty has several conditions. First, the servant must be either at work or using the chattel of the master, and second, the master must know or have reason to know that he as the ability to control the servant and the necessity and opportunity for exercising such control.[679]

The concept of negligent supervision also applies (but to a lesser extent) to independent contractors. In the contractor context, Prosser reports that "quite apart from any question of vicarious responsibility, the employer may be liable for any negligence of his own in connection with the work to be done."[680] Where there is a foreseeable risk of harm to others unless precautions are taken, it is the duty of the employer to exercise reasonable care to select a competent, experienced and careful contractor with proper equipment and to provide, in the contract or otherwise, for such precautions as reasonably proper to be called for.[681] Insofar as the employer retains any control over the work, he is required to exercise reasonable care for the protection of others.[682]

---

[676] *Id*.

[677] Operative personnel are employees, contractors or agents of a CA who have either (a) managerial or policy-making responsibilities, or (b) duties directly involving the issuance of certificates, creation of private keys or administration of computing facilities. Utah Gen. Stat. 46-3-103 (20). A licensed CA may not employ as operative personnel anyone who has been convicted of a felony or who has not demonstrated "knowledge and proficiency" in following the requirements of the statute. Utah Code Ann. 46-3-201(1)(b)-(c).

[678] Restatement (Second) Torts, § 317.

[679] *Id*.

[680] Prosser and Keeton, *supra note 4* at 510.

[681] *Id*.

[682] *Id*.

8.3.3 Negligent Maintenance of a Key

An extension of the negligent supervision theory may apply specifically to the CA's duty to supervise those personnel with whom the CA has entrusted its key. A CA, like any subscriber, appears to have a duty to safeguard its private keys.[683] Arguably, a corollary to this duty is that in entrusting its key to employees or contractors, the CA has a duty to supervise these trustees to prevent unauthorized use of the key.

Although there are no cases on point, an analogous fact pattern involving negotiable instruments has been addressed by courts and legislatures. Under the law of negotiable instruments, a holder who accepts a forged instrument bears the loss and cannot enforce the instrument against the purported maker. This is a harsh result in cases where the forgery results from the purported maker's own negligence (such as, for example, when the note maker signs a note but leaves the amount field blank). Nevertheless, early cases held that the maker of the note -owes no duty to a subsequent holder because at the time the instrument is drawn there is no contract between them.

This result was ameliorated by Section 3-406 of the Uniform Commercial Code ("UCC"), which subjects a maker to a duty of reasonable care that is owed to future note holders. Section 3-406(a) provides that "A person whose failure to exercise ordinary care substantially contributors to an alteration of an instrument or to the making of a forged alteration or the forgery against a person who, in good faith, pays the instrument or takes it for value for collection." The comments to Section 3-406 state that "By drawing the instrument and setting it afloat upon a sea of strangers" the maker or drawer voluntarily enters into a relation with later holders which justifies this responsibility.

Although Section 3-406 does not seem literally applicable to digital certificates, its underlying rationale is quite relevant and strongly suggests that a comparable duty may be applied to CAs. That is, having set the CA certificate afloat upon a "sea of strangers," the CA has a duty to use reasonable care so that its private signing key is not misused to create bogus certificates which may foreseeably cause loss among relying parties.

Various courts have had occasion to apply the principles of preclusion found in Section 3-406, including cases involving check-signing machines, which seem to be highly analogous to a CA's private key. Given that the revision of Article 3 is still somewhat of a recent development, most cases are based on former Section 3-406, which expressly required the drawee bank to act not only in good faith, but also to act "in accordance with reasonable commercial standards" in paying the check. Thus much discussion is devoted to determining whether the drawee bank, because of its own failure to act reasonably, should be prohibited from asserting preclusion as to the drawer's assertion of forgery. Nevertheless, these cases are instructive as to the issue of determining failure on the part of the drawer to exercise ordinary care.

---

[683] Utah Code Ann. § 46-3-305

Quite often where drawers are found to be negligent, their negligence will be based not only on their failure to appropriately safeguard the check-signing device, but also on their failure to exercise sufficient control over the forging employee, especially where that employee has multiple responsibilities which, in the interests of asset security, should be delegated to separate individuals. For example, in *Mid-American Clean Water Systems Inc*. a bankruptcy court applying former Section 3-406 found an employer's negligence substantially contributed to the forgery of its checks by its bookkeeper where the employer, after having employed the bookkeeper for only two months, gave the bookkeeper complete control over the day-to-day finances, allowed the bookkeeper to receive the mail everyday, and gave the bookkeeper access to both its blank checks and a rubber stamp bearing the signature of the company president.[684] Here the court took notice of the fact that even without the signature stamp the bookkeeper would have been able to carry out his scheme because of the employer's total failure to exercise sufficient control over the bookkeeper.[685] Thus the employer was precluded from asserting the forgery against the bank as a basis for recovery.[686]

A drawer will not be found negligent, however, and thus will not be precluded from asserting the forgery against the drawee bank, where there is no inadequacy of security precautions taken on behalf of the drawer to protect its signature stamp. *In Mortimer Agency, Inc. v. Underwriters Trust Co*., a drawer was found not negligent and thus was not precluded from asserting forgery against the drawee bank where, during a series of burglaries, checks were removed from the back of the drawer's checkbook, the checks were signed using the drawer's rubber signature stamp, the checkbook and signature stamp were found in their accustomed place and appeared to be left undisturbed, and the drawer promptly notified the bank of the forgeries after receiving its bank statement.[687] The court found no inadequacy in the security precautions taken by the drawer, even in light of the repeated burglaries, that would justify an inference of negligence.[688]

---

[684] *In re Mid-American Clean Water Systems Inc*., 159 Bankr. 941 (1993).

[685] *Id*. at 946.

[686] *Id*. at 948. See also Acrometal Cos. v. First Am. Bank, 475 N.W.2d 487 (Minn. Ct. App. 1991) (court stating that, if facts showed employer negligent, that negligence would substantially contribute to making of unauthorized signatures where employee with access to company's facsimile signature plate had responsibility for maintaining accounts payable, issuing company checks and reconciling bank statements, and thus bank would not be liable for money paid on checks if it acted in good faith and in commercially reasonable manner).; Read v. South Carolina Nat'l Bank, 335 S.E.2d 359 (S.C. 1985) (employer's negligence as a matter of law substantially contributed to employee's forgeries and thus precluded employer from asserting forgery against drawee bank where employer failed to maintain proper control over signature stamp, allowed same person who had possession of checkbook to reconcile bank statements without supervision or verification, and failed to examine bank statements in timely manner).

[687] *In Mortimer Agency, Inc. v. Underwriters Trust Co* 13 U.C.C. Rep. Serv. (Callaghan) 270 (N.Y. Civ. Ct. 1973).

[688] *Id*. See also First Nat'l Bank & Trust Co. v. Cutright, 205 N.W.2d 542 (Neb. 1973) (evidence of negligence on part of drawer was minimal where very old signature stamp, which had been used by legal assistant to sign letters and legal papers and had never been used for purpose of signing checks, was inappropriately used by secretary to forge checks, and where bank signature card did not authorize use of facsimile signature).

8.4 Liability for Criminal Acts of Third Party

As a general proposition, a defendant has no general duty to take precautions against the criminal acts of others or to protect a plaintiff from the criminal acts of others,[689] unless: (a) the defendant by its affirmative acts created the dangerous situations in which the plaintiff was victimized,[690] or (b) the defendant owed a duty to the plaintiff by virtue of a special relationship between the defendant and either the plaintiff or the third party criminal.[691]

8.4.1 Affirmative Action

Affirmative action cases are based on the defendant taking an affirmative act that has greatly increased the risk of harm to the plaintiff through the criminal acts of others. For example, when a defendant leaves his keys in an unattended automobile, he creates an unreasonable risk that the car will be stolen and possibly misused and may therefore be liable in negligence to a plaintiff who is injured by a thief's use of the car.[692] A recurring requirement for imposing liability on the defendant is foreseeability -- the criminal conduct must be foreseeable to give rise to a duty on the part of the defendant.[693]

8.4.2 Special Relationship

Special relationship cases fall into two categories based on whether the defendant's relationship is with the plaintiff or the wrongdoer. In the first set of cases, a defendant may have a "duty to protect" the plaintiff and in the second, a "duty to control" the wrongdoer.

Duty to protect cases typically involve the following relationships:[694]

- carrier-passenger
- employer-employee
- occupier of land-invitee
- innkeeper-guest
- custodian-charge
- landlord-tenant

Duty to control cases are generally grounded on a relationship between the defendant and the wrongdoer that gives rise to an obligation onto part of the defendant to control the criminal actor's conduct or at least warn others of the actor's propensity to do harm. Examples of such relationships are:

---

[689] *See* W. Johnson, *Tort Liability in Georgia for the Criminal Acts of Another*, 18 Ga. L. Rev. 362, 362.

[690] *Id*. at 365.

[691] *Id*.

[692] See, e.g. Hill v. Yaksin, 380 A.2d 1107 (N.J. 1977).

[693] See, e.g., Elliott v. Mallory Electronic Corp. 571 P.2d 397 (1977).

[694] See Johnson, *supra* note 51

- parent-child[695]
- employer-employee[696]
- psychiatrist-patient[697]

Prosser generally suggests that a defendant may be liable if he is in a special position to control the dangerous person or prevent the harm.[698]

[695] Restatement (Second) of Torts, § 316.

[696] See discussion in Section 8.2 above

[697] See Johnson, *supra* note 51.

[698] Prosser and Keeton , *supra* note 4 at 203.

9. STRATEGIES FOR MANAGING THE CA'S LIABILITY RISK

The following is a summary of procedures and structures that the CA can use in an attempt to manage it's liability exposure. It must be recognized at the outset, however, that the exact extent and scope of the CA's potential liability is unclear at best, and potentially catastrophic at worst. The following suggestions seek to deal with the various liability issues raised in this memoranda. They are provided with the understanding that it may not be practicable, from a business perspective, to implement all of the suggestions noted here. Moreover, in some cases, implementation of one suggestion may preclude the use of another.

9.1 Use of a Separate Entity.

In light of the uncertain nature and scope of the potential liability of a certification authority, and the extensive legislative efforts currently underway in both the U.S. and foreign jurisdictions,[699] we recommend that the CA form a separate subsidiary to operate its certification authority business. This should be done in a manner so as to insulate the CA itself from any liabilities that may be incurred by the subsidiary.

While this memorandum does not attempt to address the details of establishing such a subsidiary, two important points should be noted. First, the subsidiary should be sufficiently capitalized (and perhaps insured) for purposes of its proposed business. The issue of certification authority capitalization and insurance is a subject addressed in many of the state digital signature statutes that purport to regulate certification authorities.[700] Second, to the extent that the certificates will be issued in the name of the CA, or to the extent that the CA logo will be licensed to subscribers for posting on their web site or in other promotional materials, it will be necessary to address issues related to the use of that name or logo by the subsidiary, and whether such use makes the CA an endorser or guarantor of the activities of its subsidiary, or otherwise would render the CA liable for damages incurred by its subsidiary.

9.2 Relationship with Subscribers.

The CA should enter into a binding contract with each of its subscribers that carefully defines the nature of the relationship and the nature of the products and services to be provided by the CA, and that carefully controls and limits the extent and scope of liability to which the CA

---

[699] As of February, 1998, 43 states have either enacted or are actively considering some form of digital signature or electronic signature legislation. In addition, several bills have been introduced in Congress, and several foreign countries have enacted or are currently considering digital signature legislation. Moreover, the National Conference of Commissioners on Uniform State Laws (NCCUSL) has an active drafting committee working on a Uniform Electronic Transactions Act, and the United National Commission on International Trade Law (UNCITRAL) is in the second year of a project to develop international digital signature legislation. Over 50 countries are participating in the UNCITRAL project, and the U.S. State Department estimates that many of them will adopt digital signature legislation in 1998 or early 1999, regardless of whether the UNCITRAL project is completed. For a complete summary of electronic and digital signature legislative efforts (updated weekly) see our web site at ***www.bakernet.com/ecommerce***.

[700] *See, e.g.,* Utah Code Ann. § 46-3-201 (requires proof of sufficient working capital to obtain a license); Wash. Rev. Code Ann. § 19.34.100 (same); Minn. Stat. Ann. § 325K.05 (same).

is subject. Also, because the CA will be entering into a contract with a subscriber for, presumably, only one certificate, and because the use of that certificate by the subscriber may be rather substantial, we recommend that the contract be a formal written agreement printed on paper and signed and witnessed by appropriate officers of the subscriber.

We also recommend that the CA require formal written acceptance of the certificate by the subscriber after it has been issued. Such acceptance should be a precondition to inclusion of the certificate in a repository and to any use of the certificate by the subscriber.

In developing a subscriber agreement, consideration should be given to the following issues:

(a) Certificate Application Process - procedures should be followed by both parties in connection with the bank's application for a certificate, and quality control and security aspects should be implemented.

(b) Obligations Regarding Private Key - specify the bank's obligations to generate a key pair and to keep the private key confidential; make clear that the CA will have no access to the bank's private key; contractually provide that, as between the bank and the CA, the bank is liable for all uses of its private key prior to revocation of such key in accordance with procedures specified by the CA.

(c) Certificates - consider specifying the format of the certificate that will be issued by the CA, and the data or other information that will be included; also consider specifying the operational period of the certificate.

(d) Acceptance - clearly state the requirement that the bank accept the certificate issued to it, and specify the procedure for such acceptance.

(e) Subscriber Responsibilities - clearly delineate the responsibilities of the bank as a subscriber, including its obligation to:

- Provide complete and accurate information to the CA used for the purpose of issuing a certificate, and update and correct any such information that becomes inaccurate
- Safeguard the private keys and applicable passwords
- Request that the CA suspend or revoke the bank's certificate in the event of a compromise or other specified contingency

(f) Use Restrictions - clearly identify restrictions imposed on the use of the certificate by the subscriber and secure the subscriber's agreement to abide by those restrictions.

(g) Suspension or Revocation - specify the procedures for suspension or revocation of the certificate and obtain the bank's commitment to promptly request suspension or revocation of the certificate in the event of a compromise or other specified contingency.

(h) Renewal Procedures - to the extent new certificates will be issued to existing subscribers via a procedure other than that required for the initial issuance of a certificate, that procedure should be specified.

(i) Publication of Certificates - clearly specify the procedure that will be followed with respect to the CA's publication of subscribers' certificates in its repository.

(j) Ownership and IP Rights - clarify the CA's ownership and intellectual property rights in and to its repository and CRL, and its right to publish certificates; clarify ownership of the certificate itself.

(k) Bank Indemnity - require that the bank indemnify the CA for any damages incurred by the CA that result from improper use of the certificate by the bank, erroneous information supplied to the CA by the bank in connection with the certificate application process or any other act on behalf of the bank that may give rise to CA liability.

(l) Warranties by CA - clearly specify the warranties, if any, that the CA is willing to make, and clarify that no other warranties are made, either express or implied.

(m) Disclaimer - clearly and conspicuously disclaim all implied warranties and all express warranties not specifically incorporated in the contract.

(n) Limitation of Liability - include appropriate limitations on the CA's liability, both in terms of direct damages and consequential damages, and regardless of the cause of action.

(o) Incorporation of CPS - specify that the CA's certification practice statement, certificate policy and/or other similar documents are incorporated by reference (and subject to change at any time by the CA without notice).

(p) Termination - specify the conditions under which the agreement may be terminated by either party, and the certificates canceled.

9.3 **Relationship with Relying Parties**.

It is likely that the CA will have no direct relationship with relying parties. For example, relying parties accessing a subscriber's web site will presumably obtain the subscriber's certificate directly from that web site and will verify the authenticity of the certificate by obtaining the CA's public key imbedded in their Netscape or Microsoft Web browser. In such case, the CA will have no direct contact with the subscriber.

In some cases, it may be necessary or appropriate for the subscriber to access the CA's repository. In such case, the CA will have contact with the relying party (i.e., the relying party

will be accessing the CA's database) and will have an opportunity to enter into a contractual relationship with the relying party.

Specifically, the CA may be able to structure a procedure whereby the relying party, upon accessing the CA's repository or CRL, is required to "agree" to the terms of an access agreement (i.e. a "click-wrap" agreement) as a condition to obtaining access to the CA database. This offers an opportunity for the CA to put the relying party on notice as to the intended use of the certificate, any restrictions that apply to its use and any notices, warnings or disclaimers that the CA feels are appropriate to limit the extent and scope of its duties, obligations and potential liability. It also provides the CA an opportunity to point the relying party directly to the CA's CPS.

9.4 Certificate Structure and Format.

The structure and format of the certificates issued by the CA may also offer some opportunity for limiting the extent and scope of potential liability. For example, the *certificate policies* extension in an X.509 version 3 certificate can be used to reference an appropriate certificate policy containing restrictions as to the authorized use of a certificate. If this field is flagged as "critical," that further restricts the user's ability to use the certificate outside the scope of certain parameters.

Likewise, it may be appropriate, within the text of the certificate itself, to expressly indicate that it is subject to certain restrictions and disclaimers, and to reference the user to the certificate policy or CPS where that information can be found. However, this so-called "incorporation by reference" remains a rather controversial issue and one which may be of some questionable legal validity (especially in the case of consumers). It has been the subject of extensive debate within the UNCITRAL digital signature project and has been criticized as both unreasonable and unworkable. Nonetheless, providing an express reference to the location of the CA's CPS, coupled with a few unequivocal words indicating that certain limitations and disclaimers appear therein, may help (and certainly cannot hurt) to reduce the CA's liability exposure.

9.5 Certificate Policies and Certification Practice Statements.

Because the CA will be issuing certificates that will be used in a public or open network environment, it is important that the CA accurately define the product that it has published, specify the intended uses and appropriate reliance on the product, and set forth applicable disclaimers and limitations as to the CA's liability.

Defining the product published by the CA (i.e., its certificates, repository and CRL) involves specifying the procedures and policies employed by the CA in issuing, managing and revoking certificates so that relying parties are adequately put on notice as to exactly what has and has not been done and, therefore, are put in a position so as to accurately access the reasonableness of their contemplated reliance on the certificate. This may be accomplished through the use of a certification practice statement, certificate policy or other system rules that

put all relevant persons on notice as to the nature of the product upon which they are contemplating reliance.

9.6 Relationship with a Certificate Manufacturing Authority.

If the CA decides to outsource a significant portion of its certification authority responsibilities to a CMA, this requires that the CA accurately manage and control the services to be performed by the CMA. Specifically, because many of the services to be performed by the CMA are critical (e.g., issuing certificates, revoking certificates, managing the repository, and making a CRL available), it is important that appropriate controls are put in place to ensure that the CMA performs these tasks properly and in compliance with instructions from the CA. Moreover, because the CMA will be in control of the CA's root key and CA signing key, it has the capability to cause significant damage if those keys are misused (just as an agent in control of a business's check-signing machine could cause significant damage).

The CA should manage its relationship with the CMA with the understanding that the CMA personnel in control of the CA's private key can potentially impose great harm on the CA and the banking community. Thus, the CA should specify rigorous standards and procedures that the CMA will follow with respect to (a) personnel management and (b) physical security; and (c) procedures for using the CA's key. The CA should periodically audit the CMA to ensure that it is complying with the agreed upon measures.

9.7 Certificate Application Procedures.

In most instances where the CA may be liable to a relying party or other person, its liability will be predicated on an erroneous issuance of certificates. Accordingly, the CA's first line of defense against legal liability is to adopt a rigorous certificate application process. This process should be designed to not only ferret out impostors but to also ensure that the subscriber personnel with whom the CA deals are in fact authorized to act on behalf of the subscriber in accepting an CA certificate. While the specific procedures will need to be devised by appropriate business and technical personnel, we generally recommend the following:

(a) Require the subscriber to submit a written application including: (i) signatures of two or more corporate officers; (ii) a copy of board resolutions (certified by an appropriate officer other than the two executing the application) authorizing and empowering the application signatories to request and accept a certificate; (iii) corporate seal of the subscriber; (iv) notary acknowledgment of all signatures appearing on the application; and (v) evidence that the applicant has the right to use the trade name or trademark that is to be listed in the certificate (*e.g.*, a federal trademark registration);

(b) Conduct off-line confirmation of applicants by: (i) comparing information in the application with a third-party database; and (ii) conducting interviews via telephone (or, preferably, in person) with persons whose signatures appear on the application;

(c) Establish a secure procedure by which approved applicants can initiate an electronic certificate request; and

(d) Provide training materials to approved applicants to ensure that each subscriber is fully informed as to: (i) options for securing its private subscriber key; (ii) the consequences of compromising its private subscriber key; (iii) the potential legal effect of using its private subscriber key; and (iv) procedures for revoking the subscriber's certificate (including conditions for which the subscriber is required to revoke).

9.8 Establish Robust Revocation Procedures.

A critical responsibility of a CA is to properly revoke certificates upon request of subscribers. A revocation request usually is made under conditions for which there is a higher than normal risk that a subscriber key will be used without proper authorization. Accordingly, it is imperative that the request be fulfilled on a timely basis. Otherwise, it is possible that an impostor may use the subscriber key to effect fraud on relying parties, exposing the CA to substantial potential liability.

To ensure correct discharge of this responsibility, we recommend that the CA give special focus to its revocation procedures, with a view toward ensuring that the procedures are: (a) robust (*i.e.*, always available and easily to use); (b) redundant (*i.e.*, providing multiple channels so that if one fails, others are available); (c) reliable (*i.e.*, eliminate single point of failure; provide fail-safe mechanisms to ensure that requests are fulfilled).

9.9 Purchase Insurance.

We are aware of a several CAs who have purchased insurance to manage the liabilities discussed in this memorandum. Insurance products are currently offered or under development by a number of providers, including USF&G, Cigna and CNA. As with any insurance policy, it is important that the coverage language offered by the insurance company mesh with the special risks facing a CA. Conventional "errors and omissions" coverage may not be adequate.

9.10 Conduct a Clearance Study with Respect to IP Rights.

We recommend that the CA conduct a clearance study at least with respect to the trademark that it proposes to use with its CA services. Some consideration should also be given to patents, although a full-blown infringement study is probably not a cost-effective option, particularly if a CMA is the party responsible for managing most of the technology that is potentially subject to third party patents.

10. STRATEGIES FOR PROTECTING INTELLECTUAL PROPERTY RIGHTS

Intellectual property rights were discussed above in Section 7 from a liability perspective (*i.e.*, how the intellectual property rights of others may impose liability on the CA). This section revisits intellectual property from a different perspective, namely how intellectual property rights can be used to protect the CA's intangible assets. We focus first on subject matter that can or cannot be protected by intellectual property rights and the procedures by which the CA can acquire these rights. We then apply these general principles to the documents, brands and technologies that may be used in the CA's CA business.

10.1 Patents

10.1.1 What Does a Patent Protect?

A patent is a grant by the federal government to an inventor of the right to exclude others from making, using, selling or importing an invention.[701] In the United States, there are three types of patents: (a) utility patents (for machines and other useful inventions), (b) design patents (for ornamental designs), and (c) plant patents (for distinct and new varieties of plants).[702]

Utility patents are granted for new and useful processes, machines, articles of manufacture or compositions of matter.[703] Most things that people think of as inventions -- such as light bulbs and telephones -- are covered by utility patents. Software may be the subject of a utility patent.

A design patent is granted for a new, original and ornamental design.[704] Unlike a utility patent, its term lasts 14 years from the date of issuance. A design patent covers a design as applied to an article of manufacture. Designs in the abstract are not patentable. Typical subject matter for design patents include the shape of products, such as automobiles and toys. In recent years, design patents have been granted for icons displayed on computer screens.[705]

Utility patent protection is available for any invention that is: (a) patentable subject matter, (b) useful, (c) new, and (d) nonobvious. The patent statute defines patentable subject matter as any "process, machine, article of manufacture, or composition of matter."[706] The

[701] 35 U.S.C. § 271.

[702] Plant patent protection is available for the invention or discovery of a distinct and new variety of plant.

[703] 35 U.S.C. § 101.

[704] 35 U.S.C. § 171.

[705] *See e.g.*, U.S. Pat. Nos. D295,765 and D295,635.

[706] 35 U.S.C. § 101.

Supreme Court has interpreted this very broadly, holding that patent protection is available for "anything under the sun that is made by man."[707]

The requirement that an invention be "useful" means that it must function as described, and that it must fulfill some purpose.[708] Almost anything worth building meets the requirement of utility. Typically, the U.S. PTO only rejects inventions as "lacking utility" if it believes they are impossible to practice.[709]

The requirement that an invention be "new" (or "novel") means that the claimed invention, at the time it was invented, was not "known or used by others in this country, or patented or described in a printed publication in this or a foreign country."[710] The universe of knowledge existing at the time of the invention is called the "prior art." Generally, an invention is novel unless it is identically disclosed by the prior art, in which case it is said to be "anticipated" by the prior art.

The requirement that an invention be "nonobvious" means that the invention cannot simply be a trivial variation of the existing art. Legally speaking, an invention is "obvious" when the invention, although not identically disclosed by the prior art, differs from the prior art in such a minor way that the invention as a whole would have been obvious to a person skilled in the art at the time the invention was made.[711]

10.1.2 What Does a Patent Not Protect?

Patent law does not protect discoveries of the laws of nature, physical phenomena, algorithms or abstract ideas by themselves.[712] If there is anything patentable from such discoveries, it is the application of the law, phenomenon or idea to some new and useful end. For example, Einstein could not have patented his theory of relativity. He could, however, have patented a spacecraft based on the theory of relativity. Likewise, general ideas pertaining to methods of doing business are not considered patentable.[713] There has been much debate in recent years as to whether computer software is or should be patentable. Despite the controversy, the PTO and the courts have concluded that software-related inventions are patentable.[714]

---

[707] *Diamond v. Chakrabarty*, 447 U.S. 303, 309 (1980).

[708] *Moleculon Resp. Corp. v. CBS, Inc.*, 793 F.2d 1261 (Fed. Cir. 1986).

[709] Manual of Patent Examining Procedure ("MPEP") § 706.03(p).

[710] 35 U.S.C. § 102(a).

[711] 35 U.S.C. § 103.

[712] *Id*.

[713] *In re Wait*, 24 U.S.P.Q. 88 (1934)

[714] "Patents in Cyberspace: Impact of Recent Federal Circuit Decisions," The Computer Lawyer, January, 1995, Volume 12, Number 1, Page 1.

10.1.3 Filing Patent Applications

Patents are available throughout the world, and are issued on a country-by-country basis. Patents are obtained in the U.S. by filing a patent application with the federal Patent and Trademark Office ("PTO"), pursuant to the Patent Act of 1952.[715] Patents in foreign countries are similarly obtained by filing an application in each specific country.

Even if an invention is new and nonobvious at the time it is invented, the right to a patent will be lost forever if it is not filed within one year after the invention is first: (1) in public use or on sale in the United States, or (2) patented or described in a printed publication anywhere in the world.[716] This deadline is called the one year "statutory bar." The events that trigger the bar -- use, sale, patenting and publication -- are interpreted broadly by the courts. For example, placing a new software product onto the Internet for use or downloading by the public could in many cases constitute a triggering event with respect to any invention embodied in the software.

The statutory bar rules in foreign countries are more stringent because there is no one-year grace period. There, patent rights are generally lost if the application is not filed before the first public use or publication of the invention. However, in most countries, it is sufficient that the application was at least filed in the United States before the first public use, provided that the application is then filed in the foreign country within twelve months.

The right to a patent may also be lost if the inventor "CAndons" the invention, although this rule is rarely invoked.[717]

In sum, patent applications should be filed as early as possible because in many cases, the one-year statutory bar may be triggered without the inventor's knowledge. Thus, the longer one waits to file an application, the greater the chances that the statutory bar may expire.

10.1.4 Securing Ownership of Patents

In the U.S., a patent application can only be filed in the name of the actual inventor or inventors, and they must each sign the patent application.[718] Unless the patent application is expressly assigned by the inventors, it will issue as a patent in the name of the inventors, who own the patent jointly. An application cannot be filed without an inventor's signature, except under special circumstances, such as when the inventor is missing, dead, or refuses to cooperate with an employer or other party who is entitled to have the application filed.[719]

When a company uses independent contractors to invent technology, the contractor -- not the company -- will have legal title to patents on the technology, unless the contractor has agreed

---

[715] 35 U.S.C. § 1 *et seq*.

[716] 35 U.S.C. § 102(b).

[717] 35 U.S.C. § 102(c).

[718] 35 U.S.C. §§ 111, 115.

[719] 35 U.S.C. §§ 117, 118.

otherwise and assigned its patent rights to the company. In some cases, the company may have the right to compel an assignment, but this right may require costly litigation to enforce. Agreements with contractors should require the contractor to execute any patent applications or assignments necessary to vest title in such invention in the company. Where the contractor is a corporation or other entity, the contracting company should ensure that the contractor's employees and subcontractors are also similarly obligated to assign their inventions.

When a company uses its own employees to invent technology, the company generally owns inventions made within the scope and purpose of the employee's employment.[720] Ownership is less clear where the invention is made outside the scope and purpose of employment, such as on the employee's own time. Often, employers have written agreements with their employees delineating what inventions belong to which party. Some states, such as Illinois and California, regulate the content of such agreements to protect employees from overreaching.[721]

If an employee uses any time, material or facility of the employer in developing an invention, then the employer may have, at a minimum, a "shop right."[722] A shop right is a nonexclusive, nontransferable license to the employer to use the employee's invention. The extent of shop rights vary from state to state.

As explained above, the employer's claim to ownership of an invention is not the same thing as actual ownership. The employer must secure an assignment of each patent or patent application made in the name of its employees. Otherwise, legal title to the patent remains with the employee, and the employer may have to sue to acquire good title**.**

10.2 Copyright

10.2.1 What Does Copyright Protect?

A copyright protects "original works of authorship."[723] "Original," for purposes of copyright law, means independently created with at least a modicum of creativity.[724] Copyrightable works include literary works, musical works, pictorial and graphic works, motion pictures and other audiovisual works, sound recordings, architectural works and compilations and derivative works.[725] All such works are automatically protected by copyright from the moment they are created and expressed in a tangible medium, such as on paper or on a computer

---

[720] *Arachnid, Inc. v. Merit Indus., Inc.*, 939 F.2d 1574, 19 U.S.P.Q.2d 1513 (Fed. Cir. 1991).

[721] *See*, *e.g.*, Illinois Patent Act, 765 I.L.C.S. 1060/2.

[722] *McElmurry v. Arkansas Power & Light Co.*, 995 F.2d 1576, 27 U.S.P.Q. 2d 1129 (Fed. Cir. 1993).

[723] 17 U.S.C. § 102(a).

[724] *See, e.g., Feist Publications, Inc. v. Rural Tele. Serv. Co.*, 499 U.S. 340 (1991).

[725] 17 U.S.C. §§ 102, 103(a).

disc. The copyright owner need not use a copyright notice, register with the U.S. Copyright Office,[726] or take any other action to acquire a copyright.

Literary works include all types of software and text-based works, such as books, periodicals, manuscripts, articles, and other works expressed in words, numbers, or other symbols.[727] Thus, the CA's policy statements, CPS, manuals, and other documentation should be copyrightable literary works.

Copyright protection can also exist for compilations. A protectable compilation is "a work formed by the collection and assembling of pre-existing materials or of data that are selected, coordinated or arranged in such a way that the resulting work as a whole constitutes an original work of authorship."[728] Examples of compilations include catalogues, directories, and datses, such as the repository.

Data structures may also be protectable if the selection and arrangement of elements meet the requirements of creativity and originality. For example, in *Kregos v. Associated Press*, the plaintiff Kregos asserted a copyright in a form for evaluating the performance of baseball pitchers. The district court granted summary judgment to defendant AP on the grounds that the selection of nine statistics could not be original as a matter of law.[729] On appeal, the Second Circuit reversed the decision, holding that a genuine question of fact had been raised. The court explained that it "cannot be said as a matter of law that in selecting the nine items for his pitching form out of the universe of available data, Kregos has failed to display enough selectivity to satisfy the requirement of originality."[730]

Under *Kregos*, a certificate format could be protectable insofar as the selection and arrangement of data elements exhibits the requisite degree of creativity. However, where the arrangement is driven by functional considerations, the format will probably not be protected. For example, a format consisting of subscriber name and public key would not copyrightable, but a format consisting of 50 selected attributes about a subscriber may be. In many cases, the format may fall in between these extremes and its copyrightability will require case-by-case analysis.

---

[726] While copyright registration is not required, it is recommended for purposes of obtaining advantages under the US Copyright Act, such as statutory damages and attorneys fees.

[727] 17 U.S.C. § 101 (definition of "literary works").

[728] 17 U.S.C. § 101 (definition of "compilation"); *see also* 17 U.S.C. § 103(a).

[729] *Kregos v. Associated Press*, 937 F.2d 700 (2d Cir. 1991)

[730] *Id*. at 704.

10.2.2 What Does Copyright Not Protect?

While copyright protects the expression of ideas, it does not protect ideas, facts or data by themselves.[731] For example, the names, towns, and telephone numbers of the persons living in a certain geographic area and listed in a phone book are uncopyrightable facts.[732]

Other limited aspects of a literary work -- such as individual words and short phrases, names, titles, and slogans -- are not copyrightable.[733] Likewise, the title of a book, article, or other work of authorship is generally not entitled to copyright protection.[734] Domain names, URLs, and HTML tags (*i.e.*, hypertext links) are not copyrightable either.

Copyright does not protect functionality or systems. Under this rule, some courts have refused to protect blank forms or data structures.[735] However, a work having functional elements may still embody protectable creative expression.

Protection is not available for facts even if the fact-gatherer has expended a great deal of time, effort, and money (often referred to as "sweat of the brow").[736] Rather, it is the creativity of the collection, arrangement and selection of the compilation of the facts that gives rise to copyright.[737] As explained above, compilations such as the conventional white pages that do not meet this criteria are not protectable by copyright.[738]

---

[731] 17 USC §102(b); *Feist Publications, Inc. v. Rural Tele. Serv. Co.*, 499 U.S. 340, 111 S. Ct. 1282, 1287, 1288, 289, 1290, 1293 (1991); *Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 547, 105 S. Ct. 2218, 2224 (1985) ("no author may copyright facts or ideas").

[732] For example, in one case the defendant was free to copy the subscriber information in the Illinois Bell Telephone directory and rearrange the information into phone number or street order, notwithstanding that the telephone directory "as a whole" was copyrightable because it contained some copyrightable text and yellow page advertisements. *Illinois Bell Telephone Co. v. Haines & Co. Inc.*, 932 F.2d 610 (7th Cir. 1991). Of course, the may include contract restrictions against copying by subscribers, if it chooses, but such restrictions would only bind the subscribers and not the outside world

[733] 37 C.F.R. § 202.1.

[734] See 37 C.F.R. § 202.1(a); *Duff v. Kansas City Star Co.*, 299 F.2d 320, 323 (8th Cir. 1962); *Becker v. Loews, Inc.*, 133 F.2d 889, 891 (7th Cir. 1943), *cert. denied*, 319 U.S. 772 (1943) ("the copyright of a book or play does not give the copyright owner the exclusive right to the use of the title"); *Warner Bros. Pictures, Inc. v. Majestic Pictures, Corp.*, 70 F.2d 310, 311 (2d Cir. 1934); *Arthur Retlaw & Assocs., Inc. v. Travenol Laboratories, Inc.*, 582 F. Supp. 1010, 1014 (N.D. Ill. 1984) ("one cannot claim copyright in a title").

[735] See, e.g., *Baystate Technologies, Inc. v. Bentley Systems, Inc.*, 946 F. Supp. 1079 (D. Mass. 1996) (data structures not protected by copyright); see also *Kregos, supra* note 29 (discussion cases where blank forms are not protected by copyright).

[736] *Feist Publications, Inc. v. Rural Tele. Serv. Co.*, 499 U.S. 340 (1991).

[737] For example, in *National Rifle Ass'n v. Handgun Control Ass'n,* 844 F. Supp. 1178, 1180-1181 (N.D. Ohio 1992), the court found that the NRA's selection and arrangement of public domain information in its newsletter was mechanical and routine because it merely took all the names of Ohio Representatives, placed them in order by district number, and asterisked the names of those on certain committees. The court emphasized that there were only a few ways to compile this type of information in a manner effective to lobbying organizations. The mere fact that it took a lot of time and effort to do so was irrelevant.

[738] *Feist Publications, Inc. v. Rural Tele. Serv. Co.*, 499 U.S. 340 (1991).

10.2.3 How Can the CA Obtain Copyright Protection?

Assuming that a work is (1) copyrightable, and (2) the copyright is duly owned by the CA, what does the CA need to do to protect its rights? The short answer is -- technically, nothing. Copyright ownership arises automatically upon creation, and neither a copyright notice nor registration is technically required.[739]

However, it is advisable to take a number of steps to perfect and enhance copyright protection:

(a) The CA should consider obtaining copyright registrations for important works. Registration confers valuable benefits, such as statutory damages and attorneys fees.[740]

(b) The CA should include a copyright notice on all published material, even though the law does not require it.[741]

Finally, if the CA plans to make its software or datses available to others, it should consider doing so only under a license agreement. A license agreement would provide protections that may not be available under copyright law, such as restrictions against reverse engineering of software, as well as protecting confidential information. Of course, such licenses would only bind the parties to the license, and not the outside world.[742]

10.2.4 Securing Ownership of Copyrights

Copyright is generally owned by the individual (or individuals) who actually created the work. However, there are two exceptions to this rule:[743]

First, if a work is created by an *employee within the scope of his or her employment,* the copyright is owned by the employer.[744] However, if the individual is an independent contractor rather than an employee, the individual will own the copyright, in the absence of a written assignment.[745]

---

[739] Historically, US law required that copyright notices be displayed to avoid loss of copyright rights. However, this requirement was eliminated when the US joined the Berne Convention.

[740] With respect to software, registration will require the deposit of a certain amount of computer source code, but the Copyright Office has procedures designed to maintain trade secret protections.

[741] The basic form of copyright notice is as follows: “Copyright [year of first publication] [name of owner]” or “© [year of first publication] [name of owner]” or “Copr. [year of first publication] [name of owner].” One does not need to have a copyright registration in order to use a copyright notice.

[742] For databases or materials that are intended to be kept confidential, the CA should maintain and follow reasonable security procedures to take advantage of trade secret protection, as discussed in Section 10.3.

[744] 17 U.S.C. 101 ("work made for hire").

[745] See, e.g., *Community for Creative Non-Violence v. Reid*, 490 U.S. 730 (1989).

Trade associations such as the CA often use volunteer committees to work on major projects, which can result in uncertainty regarding the ownership of copyright rights. Thus, all volunteer members (or at least those members working on significant projects) should be required to sign a written agreement expressly assigning all copyright rights to the association. The same is true for outside consultants, freelancers and independent contractors.

Second, if a work (a) is specifically ordered or commissioned, (b) falls within one of nine specific categories (described in the footnote below),[746] and (c) is subject to a written signed agreement that states that the work is considered a "work for hire," the copyright is owned by the entity that commissioned it. All three of these requirements must be met. For example, it is not enough to merely call something a "work for hire" if the work does not fall within one of the specified nine categories.

Thus, to ensure that the CA has complete copyright ownership of the works created for it, the CA should make sure that all work done by non-employees of the CA (such as a CMA), is subject to a written contract stating that all work is deemed a work for hire and that all copyright rights are assigned to the CA.

10.3 Trade Secrets

10.3.1 What Does Trade Secret Protect?

A trade secret is any information that (1) is secret, and (2) has economic value by virtue of the fact that it is kept secret.[747] Almost any information can be a trade secret. Formulas, customer lists, datses,[748] computer software,[749] product designs, manufacturing processes, business plans, algorithms, and the like have all been protected as trade secrets so long as they possess the minimum qualifications.

Theoretically, trade secret protection can last forever, but the protection can also be lost in an instant. This is because a trade secret is protected only as long as it is kept a secret and so

---

[746] The nine categories of works subject to this work for hire rule are: (1) contributions to a collective work, (2) part of a motion picture or other audiovisual work, (3) translations, (4) supplementary works (such as illustrations, charts, tables, indexes, appendices, etc.),(5) compilations, (6) instructional texts, (7) tests, (8) answer material for a test, and (9) atlases. 17 USC §101

[747] See Uniform Trade Secrets Act § 1(3); Restatement (First) of Torts § 757, Comment b (1939); Restatement (Third) of Unfair Competition § 39 (1995). The Uniform Trade Secrets Act has now been adopted in 40 states.

[748] *MAI Systems Corp., v. Peak Computer, Inc.*, 991 F.2d 511, 521 (9th Cir. 1993), *cert. dismissed* 114 S.Ct. 671 (1994) (holding that a customer database qualifies as a trade secret).

[749] *Avtec Sys., Inc. v. Peiffer*, 30 U.S.P.Q.2d 1365, 1370 (4th Cir. 1994) ("there is no difficulty in finding the existence of a trade secret in the source or object codes to computer programs . . . ."); *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 522 (9th Cir. 1993), *cert. dismissed*, 114 S.Ct. 671 (1994); *Atari Games Corp. v. Nintendo of America Inc.*, 975 F.2d 832 (Fed. Cir. 1992); *Computer Assocs. Int'l, Inc. v. Altai Inc.*, 23 U.S.P.Q. 2d, 1241 (2d Cir. 1992), *aff'd in part and vacated in part*, 982 F.2d 693 (2d Cir. 1992); *Trandes Corp. v. Guy F. Atkinson Co.*, 798 F. Supp 284, 288 (D. Md., 1992), *aff'd in part and rev'd in part*, 966 F.2d 655 (4th Cir. 1993), *cert. denied* 114 S.Ct. 443 (1993); *S.O.S., Inc. v. Payday, Inc.*, 886 F.2d 1081, 1089-90 (9th Cir. 1989).

long as no one else duplicates it by legitimate, independent research or reverse engineering.[750] But, as in the case of the Coca-Cola formula, if proper steps are taken to preserve secrecy, trade secret protection can last indefinitely.

10.3.2 How Can the CA Obtain Trade Secret Protection?

Trade secret protection for information, like copyright and trademark protection, applies automatically to information that qualifies.[751] No legal formalities such as notice or registration are required. However, as discussed below, there is a general obligation to take steps that are appropriate under the circumstances to keep the information secret.

In addition, information may be protected by contract, even if it does not meet the technical definition of a trade secret. For example, the CA's private CA signing keys will be shared with its subcontractor CMA. Regardless of whether the signing keys are "trade secrets," the CA should contractually obligate the CMA to keep the keys secure and secret.

The trade secret laws will not protect all information. As noted above, to qualify as a trade secret, information must have two basic characteristics: (1) it must be kept secret, and (2) it must provide its owner with economic value -- such as an advantage over competitors who do not have it.

The first requirement - secrecy - may be somewhat obvious but is also of critical importance. In the absence of secrecy, there is no trade secret protection.[752] The concept of "secrecy" has two elements: (a) the information must *be* secret, that is, not known generally to the industry, and (b) the information must be treated as and *kept* secret. The first element is generally not controllable by the owner, but the second element is.

Depending upon the circumstances, fulfilling the obligation to maintain secrecy may require the owner to take affirmative steps designed to ensure that the information will remain secret.[753] This may include steps such as restricting access to persons, having a "need to know," using passwords and key codes, encrypting sensitive data, employing physical security measures like locked file cabinets, and requiring employees and others to sign confidentiality agreements.[754] When trade secret information is communicated electronically, it may be

---

[750] *University Computing Co. v. Lykes-Youngstown Corp.*, 504 F.2d 518, 534 (5th Cir. 1974), *reh'g denied*, 505 F.2d 1304 (5th Cir. 1974).

[751] See Uniform Trade Secret Act § 1(4).

[752] *Avtec Systems, Inc. v. Peiffer*, 30 U.S.P.Q.2d 1365, 1370 (4th Cir. 1994) ("the hallmark of a trade secret is not its novelty but its secrecy"); *Dionne v. Southeast Foam Converting & Packaging, Inc.*, 397 S.E.2d 110, 113, 17 U.S.P.Q.2d 1565, 1567 (Va. 1990).

[753] *Amoco Prod. Co. v. Lindley*, 609 P.2d 733, 743 (Okla. 1980).

[754] In one case, for example, a court held that software was not a trade secret because, among other things, the plaintiff never intended to keep the relevant information secret. This conclusion was based in part on the fact that when the software was installed, no policy was established to keep it secret, and that the plaintiff had allowed one of its employees to write an article explaining the system to other experts in the field. *Jostens, Inc. v. National Computer Systems, Inc.*, 318 N.W.2d 691, 700 (Minn. 1982).

necessary to require the use of secure networks or alternatively, encryption so that anyone who is able to access the message will be unable to read its contents. Trade secret information that is stored in a digital form should be kept on a secure system and/or in encrypted form.

The CA should periodically conduct an "inventory" of potential trade secrets used in connection with its CA program. Obviously, a number of elements used in the program will be known and available to the industry, such as the use of standard digital signature algorithm. However, the CA may possess or develop information that is not generally available, such as specialized software, internal methods and procedures, and confidential datses.[755] In the case of such information, the CA should implement procedures designed to keep the information secret, to avoid loss of protection.[756]

10.3.3 How Can Trade Secret Protection Be Lost?

Unlike copyright protection (which normally lasts for the life of the author plus 50 years), and patent protection (which generally lasts for up to 20 years), trade secret protection can last forever. That is why, for example, Coca-Cola chose trade secret over patent protection for its formula. However, trade secret protection is also very fragile. It is automatically lost whenever the secret is disclosed or becomes generally known within the industry. This can happen through independent discovery or unrestricted disclosure.

If someone independently duplicates a secret by legitimate independent research, it is no longer a secret, and that person is free to use or disclose it.[757] Thus, for example, someone might be able to legally reconstruct the CA's entire "secret" datse of subscriber information by copying from available sources and doing his or her own legwork.

Unrestricted disclosure of trade secret information will also result in the loss of trade secret protection.[758] This frequently occurs through simple carelessness on the part of the trade secret owner. In one case, for example, trade secret protection was lost when a company allowed one of its employees to publish an article explaining its system to other experts in the field. In addition, courts have held that an unrestricted disclosure occurs when trade secret information is posted to the Internet, even if only briefly in a newsgroup posting.[759]

---

[755] In addition, even if the individual pieces of information were available in the industry, such a ready-made compilation might not be generally available. In that case, the database itself (much like a customer or supplier list) could be a protectable trade secret, even if the individual components are not.

[756] Note that trade secret protection can exist even if the database is not copyrightable.

[757] *University Computing Co. v. Lykes-Youngstown Corp.*, 504 F.2d 518, 534 (5th Cir. 1974).

[758] *See, e.g., Advanced Computer Services of Michigan, Inc., v. MAI Systems Corp.*, 845 F. Supp. 356, 370 (E.D. Va. 1994) ("trade secret rights do not survive when otherwise protectable information is disclosed to others, such as customers or the general public, who are under no obligation to protect its confidentiality."); *Secure Services Technology, Inc. v. Time and Space Processing, Inc.*, 722 F. Supp. 1354, 1361 (E.D. Va. 1989).

[759] *Religious Technology Center v. Netcom Online Communications Services, Inc.*, No. C-95-20091 (N.D. Cal. September 22, 1995) (when plaintiff's alleged trade secrets were posted on the Internet, they lost their status as secrets).

Thus, the CA should be careful to avoid inadvertent disclosure of trade secrets by its employees or others in a confidential relationship, and should maintain appropriate security procedures for any information that is stored or communicated electronically. The contractual arrangements with the CMA should clearly specify the parties' confidentiality obligations, and the systems themselves should be designed to provide a reasonable level of practical security.

The CA, like many businesses, will need to disclose trade secrets in the course of its business, such as disclosure to programmers, consultants, joint venturers, suppliers, and in some cases subscribers and relying parties. Information will still be protected as a trade secret if it is disclosed "in confidence" -- that is, under circumstances such that the recipient is legally obligated to keep it secret.

Thus, it is critical for the CA to establish a confidential relationship with everyone who will have access to trade secret information. A confidential relationship exists when (1) the person receiving the disclosure expressly promises to keep it secret, such as by signing a confidentiality agreement, or (2) the secret is disclosed in the context of a relationship in which the law implies an obligation of confidentiality, such as an employer-employee relationship.[760]

Thus, if the CA were to disclose trade secrets to non-employees such as CMA personnel, volunteer members, subscribers, or even relying parties, it should be done pursuant to a written confidentiality agreement.

10.4 Trademarks

10.4.1 What Does Trademark Protect?

Trademarks are words, symbols or other devices used to distinguish the goods or services of one person from those of another.[761] Any number of items can constitute a trademark. The most commonly used forms of trademarks are words and phrases (such as "Xerox" and "Don't Leave Home Without It"), pictures and symbols (such as the Nike "swoosh"), numerals and letters (such as "IBM" and "Lotus 1-2-3"), and sounds and music (such as advertising jingles and television program themes). In this case, the CA may wish to market its CA services under the CA name and logo, or create a separate name or logo for the service. Similarly, the CA may wish to use the CA name and logo as a trademark to indicate the source of each digital certificate.

---

[760] See, Restatement (Third) of Unfair Competition § 41 (1995). In most states, employees are automatically bound not to disclose or use for their own benefit the trade secrets disclosed to them by their employer, so long as they have notice of the confidential nature of the information. No written contract is necessary to create this obligation. *See, e.g., Integrated Cash Management Services, Inc. v. Digital Transactions, Inc.*, 732 F. Supp 370 (S.D.N.Y. 1989) *aff'd*, 920 F.2d 171 (2d Cir. 1990); *Engineered Mechanical Services Inc. v. Langlois*, 464 So. 2d 329 (La. Ct. App. 1st Cir. 1984) *cert. denied* 467 So.2d 531 (La. 1985). *See also*, Restatement (Third) of Unfair Competition § 42 comments b and c (1995). It is often wise, however, to have employees sign confidentiality agreements in which they expressly acknowledge that the confidential information to which they have access is considered to be the employer's trade secret, and that they will not improperly use or disclose it. An employee confidentiality agreement serves to demonstrate that the employer considers its developments to be secret and valuable.

[761] Trademarks are governed by state law, as well as by a federal statute known as the Lanham Act, 15 U.S.C. § 1051 *et seq*.

To be protected, trademarks must be capable of distinguishing one party's goods or services from another. Thus generic terms such as "apples" for fruit cannot be protected as trademarks. Likewise, descriptive terms such as "quality gasoline" cannot be protected until the term develops recognition in the marketplace as a trademark. This recognition is called *secondary meaning*. Under the Lanham Act, the PTO may accept exclusive and continuous use of a descriptive mark for five years as *prima facie* evidence of secondary meaning.[762] Marks that are fanciful (*e.g.,* "Exxon" for oil), arbitrary (*e.g.*, "Apple" for computers) or merely suggestive (*e.g.*, "Playboy" for magazines) are protectable immediately upon adoption (assuming they do not conflict with a prior user's mark).

The owner of a mark has the exclusive right to use the mark in a particular market on particular kinds of goods or services.[763] Because this right is exclusive, trademarks provide consumers with a reliable indication of source.

10.4.2 How Can the CA Obtain Trademark Protection?

Like copyrights, trademark rights arise automatically - in the US, the first person to use a mark in commerce to distinguish the source of its goods or services acquires trademark rights in it.[764] No notice or registration is required (although as noted below, registration confers valuable additional protections).

Thus, by using a mark such as the CA name and logo, or a newly selected name or logo, to promote its CA services, the CA may acquire trademark or service mark rights. The CA should consider federally registering the marks it selects to identify and promote its goods and services. In the US, registration is optional, but it bestows many valuable benefits. For example, registration gives the registrant nationwide priority to its mark as of the application filing date,[765] gives the registrant valuable presumption of ownership and validity,[766] and may allow the registrant to obtain attorney fees and treble damages.[767] The Lanham Act now permits applications to be filed prior to actual use.[768] Under this provision, applicants with a bona fide intention to use a mark can reserve it ahead of time.

Internet domain names can qualify as trademarks, so long as they are used to indicate the source or origin of goods and services. For the time being, domain names are registered with a company called Network Solutions, Inc. ("NSI"). In disputes over domain names, NSI has a policy that favors holders of federal trademark registrations.[769] Accordingly, any domain name

---

[762] 15 U.S.C. § 1052(f).

[763] 15 U.S.C. § 1114.

[764] Different rules apply in some foreign countries.

[765] 15 U.S.C. § 1057.

[766] 15 U.S.C. § 1115(a).

[767] 15 U.S.C. §§ 117, 118.

[768] 15 U.S.C. § 1051(b).

[769] URL http://www.rs.internic.net.

used in connection with the CA's CA services should also be the subject of a trademark registration, if possible.

Owners of registered trademarks may give notice of their claim to a trademark by placing a notice symbol next to the mark.[770] The proper notice for marks registered with the U.S. Patent and Trademark Office is to place the symbol ® next to the mark.[771] The ® symbol may only be used for registered marks, not for unregistered marks.

Finally, we note that trademark rights are territorial, and subject to few international treaties. That means that a trademark registration in the U.S. will not adequately protect a mark in other countries. Thus, if the CA intends that its services be promoted or used in other countries, it should consider registering its marks abroad. In certain countries, trademark rights are only available by registration, and there is little or no protection for unregistered marks. Because digital networks cross national boundaries, the online use of trademarks poses difficult problems for global trademark management. Short of registration in multiple jurisdictions, it may be difficult to secure protection in the many nations where the mark may be "used."

If the CA licenses others to use its trademarks and service marks, certain technicalities must be observed to avoid losing trademark rights. In particular, every trademark license must contain provisions ensuring that the trademark owner will exercise quality control over the licensee's operations and use of the mark. This is because the purpose of trademark law is to avoid public confusion over the source of goods - if the trademark owner allows anyone to use his mark on anything, the mark would cease to be an indicator of source. Thus, if the mark is licensed without quality control, the owner may be deemed to have CAndoned the mark entirely.[772]

10.5 Candidates for Protection

10.5.1 Overview

This section will apply the principles of U.S. intellectual property law to specific aspects of the CA's CA program.[773] As discussed below, patent protection may be available for a variety of work product developed by the CA for use in its CA business. Copyright protection should extend to the CA's software programs, manuals, and textual materials such as its CPS and other policies. In addition, databases (such as of subscriber information), CRLs, and other lists could be protectable as copyrightable compilations if certain criteria are met. The keys and the digital certificates themselves are probably not protectable under copyright, although there are obviously not yet any court decisions on the subject. However, the CA's private keys and other confidential information can be protected as a trade secret or by confidential disclosure

---

[770] While notice is not required, mark owners who fail to give notice may be unable to collect damages or profits in a dispute. 15 U.S.C. § 1111.

[771] *Id*.

[772] *See, e.g*., *Broeg V. Duchaine*, 67 N.E.2d 466, 69 U.S.P.Q. 627 (1946).

[773] This memo is limited to US law. However, the US is a signatory to a number of international treaties which essentially confer copyright protection to US nationals in other countries.

agreement contract. Brands developed by the CA to market its CA services are protectable by trademark.

10.5.2 Databases

The CA will maintain directories and other databases, including a repository of issued certificates and certificate revocation lists. These databases may be protected using a three-fold strategy of copyright, trade secret and contractual licensing arrangements.

(a) Copyright. As explained above, copyright law does not protect the specific items of factual information contained in CA's databases. However, each database as a whole may qualify for copyright protection as a compilation if there is a sufficient level of originality in the selection and arrangement of the data. For example, a compilation of favorite names for children is potentially creative because there may be original artistic selection in choosing the favorite names out of all the possibilities. Further, the manner in which the names are arranged may constitute protected expression. However, not every compilation meets these criteria. For example, a standard white pages directory is not protectable because neither the arrangement (*i.e.*, alphabetical listing of names) or the selection (every telephone subscriber) is considered original.[774]

Like the white pages, there are two reasons why CA databases might not be protected by copyright. First, the CA databases are likely to follow pre-existing standard formats developed by others, thus precluding "arrangement" as a basis for the CA claiming copyrightable expression in the compilation. Second, the databases are likely to be rote lists (*i.e.*, of subscribers or revoked certificates) that do not represent creative selection. Despite these concerns, the CA should claim a copyright in its databases until such time as it affirmatively determines that they are not protected.

(b) Trade Secret. Even if CA databases are not fully protected by copyright, trade secret protection may be available if the information meets the criteria discussed above in Section 10.3. Because repositories and CRLs will presumably be made available to a large number of persons, it may be difficult to protect these materials as trade secrets.

(c) License Restrictions. Even if the CA databases are not fully protected by copyright or trade secret, the CA may be able to obtain some protection through licensing arrangements. Specifically, the CA should require any subscriber, relying party or other person who gains access to an CA database to agree that the information contained in the database will not be copied, distributed or disclosed to others except as specifically allowed by the CA. At least one federal appellate court has ruled that these restrictions are enforceable, even though they bestow copyright-like protection on uncopyrightable subject matter.[775] That case, *ProCD v. Zeidenberg*, involved a CD-ROM containing white pages listings. The CD-ROM had been licensed by the plaintiff ProCD, Inc. to the defendant (an individual) pursuant to a shrink-wrap license agreement that prohibited commercial distribution of the information. Without

---

[774] *Feist Publications, Inc. v. Rural Tele. Serv. Co*., 499 U.S. 340 (1991).

[775] *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996).

violating ProCD's copyrights, the defendant placed the listings onto an Internet Web site. ProCD sued the defendant for breaching the shrink-wrap license agreement. The U.S. Court of Appeals for the Seventh Circuit held that the shrink-wrap license agreement was binding on the defendant, and that the enforcement of its restrictions against distribution was not preempted by federal copyright law.[776]

10.5.3 Documentation

Documentation publications such as a CPS or user handbook that are used in the CA's CA business can be protected as copyrightable literary works. The procedures and other ideas outlined in the documentation will not be protected by copyright alone, however. If CA documentation is developed by independent contractors, the CA should ensure that rights to the documentation are assigned to the CA.

10.5.4 Brand Names

The brand name under which the CA markets its CA services can be protected by trademark, provided that it does not infringe the rights of a prior user. As explained in Section 10.4 above, a brand name should be the subject of a careful clearance study to avoid conflict with prior users. Also, brand names should be fanciful, arbitrary or suggestive, if practicable. Brands that are generic or merely descriptive may be impossible or difficult to protect. Once a brand name has been selected, the CA should immediately file a trademark application for the brand with the U.S. PTO.

10.5.5 Software

Software developed by or for the CA may be protected in at least three ways. Protection of user interfaces generated by software is separately discussed in Section 10.5.10 below.

(a) Patent. If the software embodies patentable invention, it may be the subject of a utility patent application. Although there is some continuing controversy about the patentablity of software-related inventions, programs can generally be patented insofar as they are applied to achieve a specific physical result (such as the creation of a digital signature).[777]

(b) Copyright. Software is protectable by copyright. Copyright notice should be applied to software in three respects: (1) in the source code; (2) in the screens displayed by the code; and (3) on the physical media, if any, that is used to distribute the software. If software is developed for the CA by contractors, the CA should ensure that rights to the software are assigned to the CA.

(c) Trade Secret. Trade secrets incorporated into the software may be protectable if they meet the criteria discussed in Section 10.3. Trade secret protection is a particularly appropriate way to protect details such as the structure, organization and algorithms

---

[776] *Id*.

[777] *See, e.g., In re Alappat*, 33 F.3d 1526 (Fed. Cir. 1994) (*en banc*)

used in software. These details are embodied in the software's human-readable *source code*. Typically, that source code is kept secret and secure. Only the machine-readable or *object code* version is made generally available. As a practical matter, it may be impossible for users to reverse engineer the software's trade secrets using only object code. To further reduce the likelihood that software will be reverse engineered, the CA should only provide the software pursuant to a license agreement that specifically prohibits decompilation or reverse engineering. However, there may be some limitations to the enforceability of such provisions, particularly in Europe.[778]

10.5.6 Content of a Particular Certificate

The data of a particular certificate by itself does not appear to be protectable by patent (because mere data is not patentable subject matter) or by copyright (because copyright does not protect facts). Conceivably, textual elements (such as a liability disclaimer) in the certificate extension fields could be independently copyrightable. On this basis, the CA could in good faith include a copyright notice in each certificate if such elements included in its certificates.

The information on a certificate could theoretically be a protected trade secret and this protection could be effectuated by requiring any party who has access to the certificate data to agree to hold it confidential. As a practical matter, however, certificates are intended to be widely distributed, so trade secret protection does not appear to be a viable option.

Overall, there does not seem to be any intellectual property right that would be squarely applicable to the content of a certificate, with the possible exception of textual elements in the extension fields. However, as between the CA and its subscribers, it may be possible to impose a contractual term where the subscriber agrees that the CA shall have the specific rights normally attendant to "ownership" (*e.g.*, the right to control the use and distribution of the certificate).

10.5.7 Format of a Certificate

The format of a certificate is conceivably protectable by copyright.[779] However, we assume that any certificate formats used by the CA will follow a pre-existing standard such as X.509. If that is the case, then the CA would presumably not be developing its own certificate formats and therefore would have no potential copyright rights. However, this question should be given further consideration if the CA develops specific protocols or coding schemes with respect to any user-defined certificate extensions.

10.5.8 CA Key Pairs

Key pairs by themselves do not appear to be covered by patent, copyright or trademark law. However, trade secret law is possibly applicable to protect the secrecy of private keys. Regardless of whether private keys are technically "trade secrets," the CA can (and should)

---

[778] See, *Atari Games Corp. v. Nintendo of America, Inc.*, 24 U.S.P.Q.2d 1015 (Fed. Cir. 1992); *Sega Enterprises, Ltd. v. Accolade, Inc.,* 977 F.2d 1510 (9th Cir. 1992); European Union Software Directive, Article 5(1), 5(3) and 6.

[779] See *Kregos*, supra note 29.

develop legally enforceable rights to the keys through appropriate contractual arrangements between the CA and any supplier or employees to whom the keys are entrusted.

Apart from intellectual property, private keys may be permanently stored in tamper proof hardware tokens. As a practical matter, property ownership of the token may amount to ownership of the key stored inside. Ownership of the token is the matter of conventional personal property law. If the CA entrusts its private keys to a CMA or another supplier, it should ensure that the supplier agrees that the CA owns the keys and all physical embodiments or containers of the keys.

10.5.9 Subscriber Key Pairs

Under at least the Utah statute, a private key is the "personal property" of a subscriber who rightfully holds it.[780] Although it may be possible for the CA and its subscribers to agree to a contrary arrangement (*i.e.*, that the CA owns the subscribers' private keys), this is probably not advisable for two reasons. First, it is impractical since it is the subscriber (not the CA) who is in sole possession and control over the private key. Second, by asserting ownership over the subscriber's private key, the CA may raise troublesome liability issues with respect to third party claims based on messages digitally signed using the key.

10.5.10 Interfaces

An interface is a connection between two devices, or between a device and a person. For example, user interfaces are the graphics and command structures presented to users of software. Interfaces also exist between hardware and software. A particularly important interface for the CA may be the Web site or other vehicle used by subscribers to request certificates or used by relying parties to access the repository or CRL. Interfaces (particularly Web sites) may have a variety of subject matter that can be protected as intellectual property.

(a) Patent. The graphic symbols (or "icons") of user interfaces can be the subject of design patents.[781] Also, the logical structure of the interface itself can be patented. For example, one patent issued to Apple Computer claims a user interface method for allowing a user to traverse a hypertext database.[782] There is some controversy about the use of intellectual property -- either patents or copyrights -- to protect interface specifications.[783] Some commentators argue that if the interface of a popular program is protected, it may be impossible for other programs to be "interoperable" with the popular program. This in turn may thwart free competition to an extent not intended by intellectual property laws.

(b) Copyright. The software and text, graphics and other material displayed as part of a user interface may be protected under copyright law. As with other copyrightable works, the CA should take appropriate steps to ensure that it owns the protected

---

[780] Utah Code Ann. 46-3-305(2).

[781] *See, e.g.*, U.S. Pat. Nos. D295,765 and D295,635.

[782] U.S. Reg. No. 5,408,655; *see also* U.S. Pat. Nos. 5,448,695 and 5,347,658.

[783] *See* J. Band and M. Katoh, Interfaces on Trial (Westview Press, 1995)

subject matter, that copyright notice is displayed and that copyright registrations are promptly filed.

(c) Trademark. The overall visual impression of the interface may be protectable as trade dress.[784] Also, any specific trademark terms used with the interface may be protected as described above. If the interface is provided on a Web site, the domain name of the Web site's URL may be protected by trademark. As explained above, the CA should select a URL that is the subject of a trademark registration, if practicable.

10.5.11 Encryption Methods and Security Procedures

Encryption is patentable and patented as explained above. While the CA will probably not develop its own encryption algorithms, it may develop related security techniques and procedures that could be appropriate subject matter for patent protection. These techniques may instead be protected as trade secrets to the extent that they are not known outside of the CA.

[784] See *Two Pesos, Inc. v. Taco Caabana, Inc*., 505 U.S. 763 (1992) (decor, menu and style of restaurant constituted protectable trade dress).