1999

The Hedgehog and the Fox: Distinguishing Public and Private Sector Approaches to Managing Risk for Internet Transactions

Jane Kaufman Winn
University of Washington School of Law

THE HEDGEHOG AND THE FOX: DISTINGUISHING PUBLIC AND PRIVATE SECTOR APPROACHES TO MANAGING RISK FOR INTERNET TRANSACTIONS

JANE KAUFMAN WINN*

"The fox knows many things, but the hedgehog knows one big thing." Archilochus[1]

TABLE OF CONTENTS

INTRODUCTION

In his essay *The Hedgehog and the Fox*, Isaiah Berlin used an ancient Greek proverb comparing these animals as a metaphor to express a deep division among thinkers and writers in their understanding of the human condition.[2] In this essay, I extend the metaphor to contrast the differing

* Associate Professor, Southern Methodist University School of Law, and author of THE LAW OF ELECTRONIC COMMERCE (3d ed. 1998 & Supp. 1999). This paper is based on a presentation the author made at the Third Usenix Workshop on Electronic Commerce, September 3, 1998 in Boston, Mass. The author wishes to thank Dwight Arthur, Walter Effross, Carl Ellison, Dan Geer, Dan Greenwood, John Gregory, and Lawrence Lessig for their comments on earlier drafts of this paper.

1. ISAIAH BERLIN, RUSSIAN THINKERS 22 (1978) [hereinafter HEDGEHOG & FOX]. This essay was originally published as "Leo Tolstoy's Historical Scepticism" in Oxford Slavonic Papers 2 (1951), citing ARCHILOCHUS FRAG. 201 IAMBI ET ELEGI GRAECI, VOL. I (M. L. West ed.) (1971).

2. *See* HEDGEHOG & FOX, *supra* note 1, at 22 (positing some individuals possess intellectual and artistic personalities that relate everything to central vision while others pursue many ends, which are often unrelated and contradictory).

approaches to risk management taken by the public sector in the exercise of its sovereign functions and that taken by members of the private sector in the conduct of commercial transactions. In light of the differences in these basic approaches to questions of risk management, I will evaluate some widely discussed models of public key infrastructures[3] for administering digital signature authentication systems. The basic model most commonly discussed today can easily be assimilated to the public sector model of risk management, but does not readily permit the incorporation of the most important features of private sector risk management models. As a result, I predict that before digital signature technology will gain widespread use in business technology, further significant progress will have to be made in the design of public key infrastructures. In addition, I argue that a public sector risk management model is not appropriate for new technology distributed by private actors unless there is a consensus that such an indirect subsidy is in the public interest generally, not just in the interest of certain private promoters of the technology. Furthermore, before the public sector adopts digital signature technology, political issues outside the scope of risk management policies will have to be addressed. For example, political issues such as the degree of protection to be granted to citizens' privacy rights within such an infrastructure will have to be resolved before a determination can be made whether the use of such a technology is genuinely in the public interest.

I. THE HEDGEHOG AND THE FOX

In his essay on Tolstoy's philosophy of history, Berlin begins with the fragment from the Greek poet Archilochus, "the fox knows many things, but the hedgehog knows one big thing."[4] The conventional interpretation of this proverb is that the fox, for all her cunning, may be defeated by the hedgehog's one defense. Berlin suggests the metaphor may also be used to highlight one of the important differences between the basic visions of life held by different thinkers and writers.[5] On the one hand there are those who believe that there exists "a single, universal, organizing principle in terms of which alone all that they are and say has significance."[6] On the other side of the divide are those whose beliefs are scattered or diffuse, moving on many levels, seizing upon a vast variety of experiences and ob-

3. There is no accepted definition of the term "public key infrastructure." In this paper, the term is used to mean any system for regulating the distribution of public keys in a networked environment.

4. HEDGEHOG & FOX, *supra* note 1, at 22.

5. *See id.*

6. *Id.*

jects for what they are without seeking, consciously or unconsciously, to fit them into any one unchanging, all embracing, unitary vision. The first kind of intellectual is like the hedgehog, the second is like the fox.[7] Berlin suggests that Dante, Plato, Lucretius, Pascal, Hegel, Dostoevsky, Nietzsche, Ibsen and Proust are, in varying degrees, hedgehogs, while Herodotus, Aristotle, Montaigne, Erasmus, Moliere, Goethe, Pushkin, Balzac, and Joyce are foxes.[8] Berlin readily acknowledges that, "like all over-simple classifications of this type, the dichotomy becomes, if pressed, artificial, scholastic, and ultimately absurd."[9] Yet he argues that because the distinction captures an important insight, it provides a useful starting point for genuine investigation.

Having set up this distinction, Berlin uses the rest of the essay to describe and analyze Tolstoy's philosophy of history, as set forth in expository passages scattered throughout *War and Peace*. Berlin believed that Tolstoy's philosophical discussions were too often dismissed by literary critics as a distraction from the brilliance of the novel, while at the same time were rarely given the recognition they deserved by academic philosophers.[10] Berlin argues that Tolstoy's life was characterized by a profound longing for a vision that would permit him, like a hedgehog, to resolve the variety of experience into one vast, unitary whole.[11] However, his philosophical and historical writings reveal that he, like a fox, was too acute in his powers of observation to be blind to the complexity of experience, and thus was unable ever to articulate a single vision that could account for life as he knew it.[12]

The distinction between the public and private spheres of law is about as plastic and unreliable as Berlin's distinction between philosophical hedgehogs and foxes, but it likewise captures an important element of truth, and offers a useful starting point for further analysis.[13] The public sphere in

---

7. *See id.* at 22.

8. Although scarcely mentioned in the essay, Marx would seem to be a hedgehog according to Berlin's description of the category. Likewise, Berlin does not categorize his own thought, but he would seem to be a fox. *See, e.g.*, ISAIAH BERLIN, TWO CONCEPTIONS OF LIBERTY (1958) (affirming value of liberal ideal of "negative freedom" or freedom from coercion and questioning value of "positive freedom" or freedom directed toward ideologically vetted ends).

9. HEDGEHOG & FOX, *supra* note 1, at 23.

10. *See id.* at 25.

11. *See id.* at 51.

12. *See id.*

13. An analysis of the history and complexity of the public/private distinction is beyond the scope of this essay. *See generally* Henry J. Friendly, *The Public-Private Penumbra — Fourteen Years Later*, 130 U. PA. L. REV. 1289 (1982) (discussing distinctions between public/private sectors). *See, e.g.*, Ruth Gavison, *Feminism and the Public/Private Distinction*, 45 STAN. L. REV. 1 (1992) (noting feminist challenges to public/private distinc-

law is understood to refer to the state — its organization, its relationships with other states and its relationships with its citizens — and the citizenry as a collective body. The private sphere is understood to refer to relationships between and among citizens acting as individuals. While the malleability of this distinction has been a matter of "public" record since at least as early as the 1948 Supreme Court decision in *Shelley v. Kraemer*,[14] the distinction nevertheless retains a considerable vitality as a heuristic device if not an immutable philosophical truth. For example, the debate surrounding the liability of on-line service providers for injury caused by subscriber's speech has required the reformulation of the line between First Amendment protections of free speech in the public sphere and the private cause of action for defamation which limits the scope of that public right.[15]

For the purposes of this essay, the public sector will refer to different governmental units acting in their capacity as sovereigns — guardians of the public interest and bearers of the police power. The private sector will refer to those arenas in which individuals, whether natural persons or legal entities, interact with each other without reference to the state except as the ultimate enforcer of legal rights and obligations. This is not to deny that many functions of the modern state do in fact take place in the private sector, such as when the state acts as a contracting party or waives its sovereign immunity from litigation with private parties, or when a traditional attribute of the public sector is placed under the control of private parties, as with the commercial operation of prisons. Rather, the focus of this paper is limited to those aspects of the public and private spheres that clearly correspond to the basic distinction sketched above, leaving for another occasion the analysis of those fact patterns where the public/private distinction is harder to draw. In addition, the consideration of the impact of sovereign

---

tion); Jurgen Habernas, *Paradigms of Law*, 17 CARDOZO L. REV. 771 (1996) (contrasting social ideal, social model, and proceduralist paradigms or images of society); Frederick Schauer, *Internet Privacy and the Public/Private Distinction*, 38 JURIMETRICS J. 555 (1998) (examining threat to individual privacy caused by onset of Internet).

14. 334 U.S. 1 (1948) (holding judicial enforcement of real property covenants as device to enforce racial segregation in housing violates Equal Protection Clause of Fourteenth Amendment even though Fourteenth Amendment applies to state action, not private conduct).

15. This issue was first dealt with in *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964), which held state libel laws that fail to provide for freedom of speech and press when conduct of a public official is criticized, violate the First and Fourteenth Amendments.

The Communications Decency Act (CDA) includes a safe harbor for on-line service providers. 47 U.S.C. § 230(a)(1) (Supp. III 1997). The safe harbor provided in the CDA was intended to overrule *Stratton-Oakmont, Inc. v. Prodigy Services Co.*, No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). The safe harbor has been upheld notwithstanding the unconstitutionality of other provisions of the CDA. *See* Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997).

actions taken in the public sphere is limited to managing the risk of financial liability for actions taken in furtherance of the public interest, not to the larger issues of how political processes can constrain the scope of sovereign authority to act.

Berlin's characterization of the hedgehog in the history of thought can be extended to the public sector, and the characterization of the fox can be extended to the private sector. The state as sovereign draws legitimacy in a modern liberal regime from its ability to express and enforce the will of the public. The state must view the individual interests of the citizenry from the commanding heights of the interests of the public as a collective entity. When the state, as sovereign, articulates and acts upon this idealized collective will, like the hedgehog, it is integrating the diversity of human experience into a single, unified vision. Individuals and groups acting within the private sector are never expected to achieve such heights of synthesis. Individuals, like the fox, are expected to be acute observers of specific data, and to use that more partial and narrow vision to operate in the fractured, pluralistic world of the private sector. Unlike the sovereign, who is expected to administer the state in the interest of all subjects without discrimination, an individual acting in a private capacity is expected to discriminate among other individuals and establish relationships selectively after evaluating the information gathered from the individual's more focused, particularistic perspective.

The risk that the sovereign will fail to execute effectively the public will, and the risk that private parties will fail to achieve the objective of their actions, may not be thought of as commensurate risks because the consequences of those failures are not normally equivalent. Failure by the sovereign to advance the public interest is not normally actionable within the courts maintained by that sovereign. If it is actionable, the remedy may be some change in the behavior of the sovereign, not monetary damages. For example, the writ of mandamus permits an individual to seek the aid of one government office in compelling another, subordinate government office to carry out its duties. In other cases, the only appropriate recourse may be to engage the political processes to modify the legal framework that constitutes the sovereign, rather than to seek compensatory redress within the existing framework. Failure by a private party to fulfill a private obligation normally is actionable within the legal system, and under Anglo-American principles of compensation, usually results in an award of monetary damages for the injured party.

At first glance, failure to comply with the applicable rules seems to give rise to quite different consequences for the malfeasor, depending on whether the malfeasor is acting in the public or private sector. Nevertheless, the rule of sovereign immunity from suit can be described as a loss

allocation rule equivalent to the loss allocation rules that apply to private parties. As a consequence of the sovereign's general immunity from suit for monetary damages, the sovereign is permitted to externalize, onto individual members of the public, the financial costs of the sovereign's failure to accomplish its objectives. Although the sovereign may generally be immune from a duty to compensate financially injured parties for the harm they suffer at the hands of the representatives of the sovereign, the sovereign can still be sanctioned through political processes for failure to fulfill its objectives. In deference to this prospect of political sanctions, a sovereign will allocate some level of resources toward dealing with particular matters within its authority. The amount of government resources allocated to addressing public concerns need not be calculated with reference to estimates of the number or amount of individual claims that might be made against the sovereign in the absence of immunity, but is more likely to reflect the outcome of political processes and constraints. In the absence of an insurance system, private parties generally will not have the same prerogative simply to cap their investment of resources to solve particular problems, and externalize onto other private parties the cost of any miscalculation. Private parties as a result must adopt more sophisticated strategies for managing the risk that their action or inaction will give rise to some harm to another party that will require financial compensation.

Just as the hedgehog's totalizing vision bears a relationship to the hedgehog's single defense against danger, the classic public sector approach to risk management bears a relationship to the general view of society the sovereign is expected to take in a republic. The sovereign hedgehog evaluates the entire complex of factors related to its exercise of authority and allocates a given level of resources to fulfill its mission in that regard. Even when it becomes apparent that the sovereign hedgehog underinvested in managing a specific risk of harm, the state will not be assigned liability for that failure, although if the harm is serious enough the state may administer disaster relief. For example, in the aftermath of the savings and loan crisis in the 1980s, state and federal regulators were not required to compensate those who suffered losses as a result of those failures that were not covered by insurance schemes. The Resolution Trust Company did use public funds to clean up the mess, but the premise for those expenditures was general economic disaster relief, not compensation for regulator negligence. By contrast, the private fox not only sees life in all its complexity, it also has a wide array of strategies for meeting the challenges of life. Private sector risk management strategies may be more partial or limited than in the public sector, but are also more diverse and tailored to specific contexts.

This fundamental distinction in approaches to uncertainty has important consequences for the design of information systems intended to manage risk. Current designs for public key infrastructures correspond to the relatively simple risk management strategies of the sovereign hedgehog. If the public key infrastructure is designed and operated to advance the public interest, then there is no conflict between the objectives served by the public key infrastructure and the risk management strategy it incorporates. If those designing and operating public key infrastructures are doing so in furtherance of private interests, however, granting the functional equivalent of sovereign immunity to certificate authorities[16] may be a poor risk liability allocation model. The large amount of uncertainty surrounding the actual degree of risk of financial losses associated with the design and operation of public key infrastructures has led to pressure for legislation shifting those risks away from those designing and operating the systems to end users of those systems. Proposals for liability limitations take two basic forms: protection for infrastructure providers and protection for parties wishing to rely on information provided through a secure system such as a public key infrastructure.[17] The quid pro quo for sovereign immunity from private sector liability rules should be a commitment to acting in the public interest and amenability to political processes. It is not clear that a political consensus has emerged to support the development of public key infrastructures for private transactions without regard to what, if any, costs are

16. *See* RITA C. SUMMERS, SECURE COMPUTING: THREATS AND SAFEGUARDS 214 (1997) (defining certification authority as entity where users of computer systems register individual "public keys" which grant them access to that computer system).

17. Examples of liability limitations for infrastructure providers include the Utah Digital Signature Act, UTAH CODE ANN. § 46-3-101 (1998), and the INFORMATION SECURITY COMMITTEE, AMERICAN BAR ASSOCIATION, DIGITAL SIGNATURE GUIDELINES (1996) [hereinafter ABA DIGITAL SIGNATURE GUIDELINES].

Examples of liability limitations for relying parties include: The National Conference of Commissioners on Uniform State Laws, *Proposed Uniform Commercial Code Article 2B: Computer Information Transactions* (last modified Feb. 1, 1999) <http://www.law.upenn.edu/bll/ulc/ucc2b/2b299.htm>; United Nations Commission on International Trade Law (UNCITRAL), Working Group on Electronic Commerce, *Draft Uniform Rules on Electronic Signatures* (visited Apr. 23, 1999) <http://www.uncitral.org/english/sessions/wg_ec/wp-73.htm>; and European Union draft directive on electronic signatures, *Electronic Commerce: Commission proposes electronic signatures Directive* (last modified May 13, 1998) <http://www.europa.eu.int/comm/ dg15/en/media/infso/sign.htm>.

There is evidence that the limited liability approach is losing favor. *See, e.g.*, National Conference of Commissioners on Uniform State Laws, *Uniform Electronic Transactions Act* (last modified June 22, 1999) <http://www.law.upenn.edu/library/ulc/ulc.htm>; *Australian Draft Electronic Transactions Exposure Bill* (visited Apr. 23, 1999) <http://law.gov.au/ecommerce/>.

externalized onto individual members of the public.[18] If prospective promoters of public key infrastructures are unwilling to bear some or all of the liability to compensate other parties harmed as a result of contact with their public key infrastructures, then the appropriate conclusion to draw may be that the technology of digital signature certificates are not yet be ready for large scale public adoption, not that the promoters should be shielded from liability.

The appropriate way to determine whether promoters of public key infrastructures should be sheltered from liability to third parties is to first articulate what public interest is served by the operation of public key infrastructures. If the public interest served is great enough, and there are no other risk management strategies available to minimize the dislocation caused by adopting this new technology rather than just shifting losses from one party to another, then the hedgehog risk management model may be sound as a matter of public policy. It is not clear, however, that there is any compelling public rather than private interest in the speedy rollout of this technology. Such haste is particularly inappropriate if more sophisticated models for implementing this technology are currently under development that may be able to minimize losses rather than simply shift them onto a party with no ability to insure or pool risks. More sophisticated models for integrating public key infrastructures into communication and information systems are in fact under development which may permit the application of more traditional private sector risk management techniques, eliminating any need for a simple rule of immunity from liability for private parties deploying this technology.

The problematic nature of changing the loss allocation rules that apply to the use of this technology is equally apparent when the deployment of public key infrastructures for indisputably public purposes is considered. Assume for the sake of argument that a political consensus has emerged that this is an appropriate technology for regulating access to pornography over the Internet.[19] In the midst of the industrial revolution, there may have been no alternative to using immunity from tort liability as a subsidy to implement a public policy favoring a particular industry.[20] In the midst of the

18. This externalized cost is the "Grandma picks a bad password and loses her house" scenario first identified as a risk of poor public key infrastructure design by Bradford Biddle and Michael Froomkin.

19. *See* Lawrence Lessig & Paul Resnick, *The Architectures of Mandated Access Controls* (visited June 6, 1999) <http://www.si.umich.edu/~presnick/papers/lessig98/index.html> (presented at Telecommunications Policy Research Conference Sept. 1998) (proposing an abstract model for mandated access controls to Internet Web sites).

20. It has been argued that changes in nineteenth century tort law made it more difficult for individual plaintiffs to recover from industrial enterprises, such as railroad companies. *See generally* MORTON J. HORWITZ, THE TRANSFORMATION OF AMERICAN LAW, 1780-1860

information revolution, it may be possible to avoid such gross forms of indirect subsidy to favored enterprises that come with the attendant risk of unacceptably high costs for individuals. The more sophisticated models for managing the risks of on-line authentication technology that are now being developed in the private sector may also hold the answer for managing the risks associated with using such technologies in the public sector. Until it is clear that such solutions are not viable, especially if a political consensus supporting the public sector use of such technologies does not, in fact, yet exist, there should not be a rush to lock in liability rules that discourage even public sector parties from developing and deploying sophisticated risk management strategies.

II. PUBLIC SECTOR RISK MANAGEMENT

Sovereign immunity is a legal doctrine that prevents a sovereign from being haled into the very courts that the sovereign provides, unless the sovereign has consented. The doctrine originated in the distant past of modern state legal systems before the notion of separation of powers had been articulated. If all the powers of government resided in one person, that person could not very well be expected to both hear and defend complaints against the sovereign.[21] While this justification is no longer very compelling, more modern ones have been developed to supplant it. In the nineteenth century, the Supreme Court concluded that sovereign immunity is justified as it defends the public interest rather than the government's interest.[22]

The protection of sovereign immunity can be waived, and in the United States many statutes waive governmental immunity to liability for torts. For example, the Federal Tort Claims Act (FTCA)[23] permits suits against the United States for state negligence torts committed by federal agencies

---

(1977) (detailing evolution of law as industrialization began in the United States). The difficulty of recovery as a plaintiff against the railroad companies is an example of a disguised subsidy to such industry. *Id.*

21. Blackstone stated the principle as "the King can do no wrong." WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 238-39 (1992).

Alexander Hamilton asserted that "[i]t is inherent in the nature of sovereignty not to be amenable to the suit of an individual without its consent." THE FEDERALIST NO. 81, at 248 (Alexander Hamilton) (Roy P. Fairfield ed., 1981); *see also* Kawananakoa v. Polyblank, 205 U.S. 349, 353 (1907) ("[A] sovereign is exempt from suit, not because of any formal conception or absolute theory, but on the logical and practical ground that there can be no legal right as against the authority that makes the law on which the right depends.").

22. *See* The Siren., 74 U.S. 152, 154 (1868) (concluding there could be possible damage to interests of citizenry as a whole caused by lawsuits brought by private citizens interfering with orderly operation of government).

23. 28 U.S.C. § 1346(b) (1994 & Supp. III 1997).

and agents. The FTCA exposes the United States to liability for money damages for the negligence of its employees in "circumstances where the United States, if a private person, would be liable to the claimant in accordance with the law of the place where the act or omission occurred."[24] In 1998, the FTCA was amended to provide that if an official is "acting within the scope of his office or employment," he has absolute immunity from common law tort liability, therefore, a suit against the federal government under the FTCA provides the exclusive remedy.[25] The FTCA contains numerous exceptions, including the "discretionary function" exception, which precludes a suit against the United States "based upon the exercise or performance or the failure to exercise or perform a discretionary function or duty on the part of a federal agency or an employee of the Government, whether or not the discretion involved [is] abused."[26] In formulating this exception, Congress sought to prevent its limited waiver of sovereign immunity from interfering with governmental policymaking.[27] So while in many specific situations the government may be liable in suits with private citizens, the general principle of sovereign immunity remains intact.

Because the doctrine of sovereign immunity shelters those who act on behalf of the state from suffering many of the adverse consequences of the decisions they make, risk management strategies used by public sector entities with regard to the exercise of their sovereign functions differ greatly from risk management strategies used by actors in the private sector who enjoy no such immunity. In executing laws and policies developed to further the public interest, governmental units define the approach they will take and allocate a finite amount of resources to solve the problem. For example, with regard to maintaining the safety of those traveling on public roads, state and local governments will allocate a certain amount of resources to developing and administering driving tests and a certain amount of resources to police and state highway patrols to monitor the conduct of drivers. The standards developed are supposed to be impartial and nondiscriminatory in light of the public purpose they are designed to further. To pursue the driver's license example, state governments issue drivers' licenses to teenagers who meet the minimum standards of competence even though it is possible to predict as a statistical matter that those teenagers may commit more motor vehicle offenses or accidentally cause more harm to others than older drivers.

---

24. *Id.* § 1346(b).

25. *Id.* § 2679(b)(1).

26. *Id.* § 2680(a).

27. *See generally* Note, *Government Tort Liability*, 111 HARV. L. REV. 2009 (1998) (discussing government tort liability and effects on policymaking).

Should later experience show that the quantity of resources allocated to achieving a particular public purpose was inadequate, the governmental unit will not normally be liable for monetary damages for its failure to achieve its stated objective. Continuing with the driver's license example, someone injured in a car accident can generally sue any person whose negligence contributed to the accident, and can even sue the governmental unit charged with maintaining the road if the failure to do so contributed to the accident and the governmental unit has waived by statute its sovereign immunity. The injured party cannot sue the state department that issued the liable party's driver's license for failure to discover that driver's incompetence, however. Similar examples could be drawn from other police powers exercised by the state, such as law enforcement building or health code compliance, or regulation of different industries.

The consequences of miscalculations in resource allocations by public sector actors are felt primarily in the political sphere, not in litigation. When sovereign power to allocate resources is exercised by elected officials, the recourse for people unhappy with the officials' decisions is political rather than legal. For example, New Yorkers who are less concerned than Mayor Rudolph Giuliani with the lack of civility in New York or with problems such as jaywalking, or who believe that law enforcement agencies should not in any event be directing significant amounts of time and energy to addressing those problems, can ridicule his campaigns in the mass media or try to vote Giuliani out of office.[28]

III. PRIVATE SECTOR RISK MANAGEMENT

With the abolition of debtors' prisons and slavery in the nineteenth century in the United States,[29] the only recourse an individual generally has against another for failure to fulfill a private obligation is an action against that other person's property. Misconduct of a nature so serious as to entail the possibility of criminal prosecution is within the exclusive competence of the state to punish[30] and, in modern legal systems, is outside the scope of

28. *See, e.g.*, Norimitsu Onishi, *Giuliani Crows as Theft Suspect Is Caught on Jaywalking Charge*, N.Y. TIMES, Feb. 21, 1998, at B1 (commenting on Mayor Giuliani's civility campaign).

29. *See generally* PETER J. COLEMAN, DEBTORS AND CREDITORS IN AMERICA 1 (1974) (explaining relations between debtors and creditors within certain regions around the United States); Charles Jordan Tabb, *The Historical Evolution of the Bankruptcy Discharge*, 65 AM. BANKR. L.J. 325 (1991) (discussing bankruptcy law in United States, including advent of permanent federal bankruptcy law in 1898).

30. At English common law, there was initially no clear distinction between the right of the sovereign and the right of the citizen to prosecute crimes. The right of private criminal prosecution was not abolished under English law until 1819. *See* 59 Geo. III, c.46

private sector liability rules. The consequences of a party to a contractual transaction failing to fulfill its obligations may give rise to a right for monetary compensation or equitable relief, but where the subject of the contract is a commercial matter, the value of equitable relief can be converted to monetary terms with relatively little loss of meaning. As a result, the ultimate consequences of different possible outcomes that must be analyzed in order to perform risk management in the private sector can be expressed in terms of financial values.

Unlike a government agency acting in its sovereign capacity, actors in the private sector will not be able to externalize onto the public the costs associated with failed endeavors. While the rigor of liability regimes varies across the spectrum of private obligations based in tort and contract law, as a general principle, private actors will be expected to bear the costs associated with their failures. If a private party is uncertain or concerned about the magnitude of costs that may result from a particular course of action, the private party has an array of risk management techniques available to guarantee its ability to meet those obligations no matter what the outcome of its conduct.[31]

In a system in which obligations are voluntarily assumed, as they are in commercial transactions, private parties are expected to estimate the costs and benefits associated with particular courses of conduct, and undertake a course of conduct only when the expected benefits are greater than the expected costs. Risk management is practiced both at the level of the individual act and at the level of aggregates of individual acts. If an individual person seriously miscalculates the risks of certain acts or a course of conduct, creating financial obligations in excess of the individual's ability to pay, the individual may ultimately be able to externalize some of his or her losses onto individual claimants by obtaining a bankruptcy discharge of those obligations. For a legal entity such as a corporation, the ultimate consequence of failing to calculate correctly the magnitude of risk associated with a particular act or course of conduct may be the termination of the legal entity. The liquidation and winding up of a corporation will also externalize the consequences of the corporation's failure to meet its obligations onto the creditors of the corporation. Unlike a sovereign, however, a corporation may not be permitted another chance to solve the problem after externalizing the costs of its earlier unsuccessful attempts. For businesses unable to reorganize their liabilities, the consequences for failure to manage

---

(1819).

31. These range from simply refraining from taking the risky act, to setting aside sufficient resources to cope with the worst possible outcome should it materialize, to participating in an insurance system or other risk pooling scheme.

risk successfully is the termination of the private entity, forcing stakeholders to realize the loss of their interests in the venture.

Laws imposing liability are among the factors private parties must take into account when attempting to estimate and manage risk, as are estimates of how markets and individuals will behave in the future. In a market-based economy, because private parties must bear the consequences of their actions, they are normally allowed wide latitude to establish their own criteria for evaluating risk and act in light of that evaluation. By contrast, common carriers are required, as a condition of receiving their franchise, to post nondiscriminatory terms on which they will conduct business and to accept anyone who meets the basic requirements for a transaction.[32] Outside the realm of business franchises imbued with a public purpose, such as common carriers, or situations where fundamental values from the public sphere spill over into the private sphere, such as civil rights laws that prohibit discrimination in private sector transactions in employment, housing, and other areas, private parties are expected to develop criteria that permit them to discriminate between risks they are prepared to accept and those they are not.

In a market economy, private parties that develop criteria that estimate risk accurately will enjoy a higher rate of return on invested resources than those who are less successful at estimating risk. While the probability of particular outcomes at the level of the individual transaction may be difficult to estimate, the probability of particular outcomes becomes much more predictable when transactions are aggregated into groups. Unlike the sovereign, who is expected to serve the public found within the sovereign's territory, parties acting in the private sector are generally permitted to pick and choose which risks are added to the pool. Risks that cannot be avoided can often be hedged by voluntarily entering into an offsetting transaction with the opposite risk characteristics. In a modern economy in which private parties no longer act based on personal relationships or in face-to-face encounters with other parties, profitability will accrue to parties that develop better formal criteria for selecting desirable risks out of large numbers of possible transactions, monitoring and pooling those risks once they have been selected, and finding strategies to hedge risks that cannot be avoided.

Automated risk management is at the heart of electronic commerce, whether that electronic commerce takes place over closed, proprietary networks of computers, or open, public networks such as the Internet.[33] The

32. 13 AM. JUR. 2D *Carriers* § 178 (1964) (noting non-discrimination requirements for common carriers).

33. *See generally* Jane Kaufman Winn, *Open Systems, Free Markets, and the Regulation of Internet Commerce*, 72 TUL. L. REV. 1177 (1998) (comparing closed and open net-

use of the Internet or other open data networks in commercial transactions offers the possibility of greater network economies and lower communication and information processing costs than were possible with an earlier generation of closed, proprietary data networks and mainframe computer systems. If problems created by the lack of security of Internet communications can be resolved, then the Internet may eventually displace existing computer networks that support large-scale electronic commerce systems such as financial markets. Financial institutions, such as banks, have been at the forefront of developing formal models to evaluate risk and manage portfolios of transactions in part because financial market values can be represented mathematically more easily than the values in some other types of commercial transactions. Part of the promise of the next generation of electronic commerce business applications is that a similar process of standardizing terms for transactions will take place as communication and information processing costs fall, and the kind of liquidity and transparency now characteristic of mature financial markets will spread to other markets. If electronic commercial practices can gain acceptance across a wide range of markets, then market participants of all descriptions will benefit from lower transaction costs.

IV. COMMERCIAL PUBLIC KEY INFRASTRUCTURE DESIGN TO DATE

Commercial transactions cannot take place without systems in place to manage not just the risks of changes in market conditions, but also the risks of fraud and error. In the world of paper-based commerce, those systems are provided in large part by accounting principles and business administrative policies. Some of those principles and policies will be used for the same purposes in electronic commerce; however, new elements will have to be added to those systems because electronic commerce involves new risks compared to traditional paper-based administrative systems. Certain types of fraud and error are more difficult to detect and control in electronic environments than in environments where administrative processes rely on paper and face-to-face interactions. In addition, electronic commerce cannot be conducted over open computer networks such as the Internet unless some system is put in place to control the threats to system security associated with open network communication systems.[34]

---

work electronic commerce).

For a discussion of the importance of risk management processes in electronic commerce see Dan Geer, *Risk Management Is Where the Money Is*, 20 THE RISKS DIGEST 6 (Nov. 11, 1998) <http://www.catless.ncl.ac.uk/Risks/20.06.html>, and David G. Masse & Andrew D. Fernandes, *Economic Modelling and Risk Management in Public Key Infrastructures* (last modified Apr. 15, 1997) <http://www.chait-amyot.ca/docs/pki.htm>.

34. *See generally* FRED B. SCHNEIDER, TRUST IN CYBERSPACE (1999) (implying role of

Some of the risks associated with open network communication systems must be managed at the level of network security, and some must be managed at the level of communication security.[35] At the level of network security, the network architecture must be designed to provide certain security services, such as authenticating users of the network, controlling access to the network, preserving the confidentiality of sensitive information associated with the network, preserving the integrity of information communicated or stored within the network, and a system to provide for non-repudiation of authenticated communications.[36] For example, the use of a "firewall" is often a part of the network security architecture, which screens all traffic directed at the network and permits only traffic that meets network security standards to pass through it and enter the network.[37] Communication or message security issues are among the network security issues that must be resolved in designing a secure system. These communication securities issues include establishing trustworthy procedures for authentication of messages, guaranteeing the integrity of messages, and non-repudiation of messages.

One technology that can be used as part of communication security is asymmetric, or "public key" cryptography[38] deployed within a system, or infrastructure, that permits its use over a network. Public key cryptography involves the use of two separate but related cryptographic keys for encrypting and decrypting text. One key is kept private and held by a single party, while the other key may be distributed publicly to anyone in communication with the individual holding the private key. The keys need not be used to encrypt the entire document because by encrypting only a hash or digest, representing the entire message, a digital signature may be produced with the private key. The party receiving the "signed" message may use the sender's public key to decrypt the message digest, and by comparing the decrypted message digest with a second digest generated by the recipient of the message, determine whether the message has been modified

---

government in protecting public welfare requires building trustworthy networked information system).

35. *See* SUMMERS, *supra* note 16, at 466-68 (noting differences between communications security and network security such as communications security focusing more on protecting integrity of "transmitted information," while network security takes into account entire network, as well as issues of authentication and cryptography).

36. *See id.* at 472 (describing security services provided by network security systems).

37. *See id.* at 506 (providing description of term firewall as a barrier "built around a network or subnetwork to protect it from the outside").

38. For a general description of public key cryptography see for example, WARWICK FORD & MICHAEL S. BAUM, SECURE ELECTRONIC COMMERCE: BUILDING THE INFRASTRUCTURE FOR DIGITAL SIGNATURES AND ENCRYPTION (1997), SIMSON GARFINKEL & GENE SPAFFORD, WEB SECURITY AND COMMERCE (1998), and BENJAMIN WRIGHT & JANE WINN, THE LAW OF ELECTRONIC COMMERCE § 3.06 (3d ed. 1998 & Supp. 1999).

with since it was signed. If the digital signature is verified in this manner, the recipient knows not only that the message has not been altered, but also that the message could only have been signed by someone with access to the private key associated with the public key used to decrypt the digest. So long as the recipient is certain that only one natural person can gain access to the private key, then the material world identity of the holder of the private key can be associated with the message in much the same manner that a manual signature made on paper with a pen associates a natural human being with the text of the paper document.

In a world in which face-to-face communications are not feasible, a system must be designed to distribute public keys so that holders of public keys feel confident that they know the material world identity of the person controlling the associated private key. One element of such a system might be a trusted third party who distributes keys to end users. If the procedure whereby the trusted third party binds a material world identity to a pair of cryptographic keys is the issuance of a certificate that includes the public key of the key pair, this trusted third party may be called a Certificate Authority (CA).[39]

A system within which public keys are distributed is often referred to as "public key infrastructures" (PKI)[40] and are designed to constrain the costs associated with using public and private keys to minimize the risks of fraud and error. The most widely known model of a PKI is based on the model of a telephone directory.[41] This model was first advanced by two of the developers of asymmetric cryptography, Whitfield Diffie and Martin Hellman in a paper published in 1976,[42] and expanded with the notion of "certificates" by a paper written in 1977 by Loren Kohnfelder, then an undergraduate at MIT.[43] If a PKI operates in the same manner as a telephone

39. A CA may also bind a pseudononymous identity to a key pair, or a role. In a closed "public key infrastructures" (PKI), the CA may not be a third party, but may be one of the two parties in communications. E-mail from Dwight Arthur to Jane Kaufman Winn (Apr. 20, 1999) (on file with author).

40. The term is often associated with specific designs for distributing public keys, such as the system described in the ABA DIGITAL SIGNATURE GUIDELINES, *supra* note 17, at 24. However, the idea of a "web of trust" associated with the use of Pretty Good Privacy (PGP) encryption program might also be described as a PKI since PGP is based on asymmetric cryptography. *See* GARFINKEL & SPAFFORD, *supra* note 38, at 213 (describing PGP and "web of trust").

41. *See* Joan Feigenbaum, *Towards an Infrastructure for Authorization*, Position Paper, 3RD USENIX WORKSHOP ON ELECTRONIC COMMERCE (Sept. 1998).

42. Whitfield Diffie & Martin Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, IT-22 (1976).

43. Loren M. Kohnfelder, Towards a Practical Public-Key Cryptosystem (1978) (unpublished B.S. thesis, Massachusetts Institute of Technology), *cited in* Rohit Khare & Adam Rifkin, *Weaving a Web of Trust* (last modified Nov. 30, 1997) <http://www.cs.caltech.edu/

directory it serves to associate a signature verification key with a name in a directory, so that someone verifying a digital signature can look up, in a directory, the public key used to verify the signature to find the name of the person associated with that key. A great deal of time and attention has been focused on the issues associated with building a reliable PKI based on this model. The problems associated with deployment of this model include complex issues of cross certification and hierarchies of certification, as well as issues associated with the issuance and revocation of certificates.[44]

The primary shortcomings of the telephone directory model of PKI as deployed in commercial settings may not be at the technical level, however. Rather, it is unclear whether such a directory, even if successfully designed and deployed, would ever be adequate to support the development of new forms of electronic commerce over the Internet. Transactors in the material world do not make the decision to execute a transaction because they have found the counter-party's name in a telephone directory, and merely knowing that there is some connection between a person and a public key will not be enough to permit electronic commercial transactions to go forward. The value of telephone directories and telephones in the material world derives in part from the fact that the function of telephones is well understood. A telephone number was usually associated with a particular telephone with a fixed location connected to the network by metal wires, and that fixed location was usually at an address that corresponded to a specific individual, family, or organization that was already known to the person using the directory.[45] Digital signatures do not have any commonly recognized association with roles in the material world. The design of user interfaces and access controls has not advanced to the point where the association of a natural human being with a digital signature can be accepted with confidence. Even if the name of a human being can be reliably associated with a digital identifier, there is not yet any system for managing the risk that more than one human being can be the legitimate bearer of that name.[46]

Commercial transactions will be executed by the parties when the risks associated with the transaction can be identified and managed, which will

---

~adam/local/trust.html> at n.37.

44. *See generally* FORD & BAUM, *supra* note 38.

45. *See* Feigenbaum, *supra* note 41, at 17; *see also* E-mail from Carl Ellison, Senior Security Architect, Intel Corporation, to Jane Kaufman Winn, Associate Professor, Southern Methodist University School of Law (Jan. 17, 1999).

46. The reader may confirm the magnitude of this problem by typing his or her first and last name into an on-line telephone directory such as http://www.switchboard.com. For most individuals in the United States, this will produce a long list of listings of individuals around the country with the same first and last names.

require more information than the mere association of a name with a digital identifier. Transacting parties will need to identify and mitigate the risks associated with the various ways a counter-party may fail to perform as expected, including the risk of financial or credit default that the non-financial elements of the transaction will not meet the parties expectations due to a breach of warranty, or that the parties are subject to the jurisdiction of courts in a remote location or subject to laws that produce surprising results when applied to this transaction. The risk that the counter-party is not who it appears to be, or that the counter-party lacks the authority or competence to enter into a binding agreement regarding the terms of the transaction, is one of the performance risks that must be identified and managed, but clearly not the only one, or even the most important one, in all transactions.[47]

At present, the practical value of digital signature certificates for commercial transactions conducted in open network environments such as the Internet is extremely limited because certificates contain so little information. The information cannot be updated once the certificate is issued, and the information that is contained in certificates may be of uncertain value.[48] One way that this technology can be adapted to meet actual commercial needs is to design a PKI for use within a closed system. Within a closed system, the meaning of digital signature certificates can be defined with sufficient rigor and access to private keys may be controlled effectively enough to permit parties to act in reliance on a verified digital signature. Information not available within the certificate can be accessed by members of the closed system through other means. In effect, the addition of a PKI to an existing closed business information system, populated exclusively by parties with prior business relationships, supports improved access controls within the closed system. This addition does not represent a radically new approach to electronic commerce, even if communications within such a closed system uses Internet networking protocols, however. The more ambitious promoters of PKI as an Internet electronic commerce solution have a more open model for PKI use in mind, which would support the execution of transactions between parties with no preexisting relationship over the Internet functioning as an open public network, not as a virtual private network or extranet.

The first attempt to establish the meaning of a digital signature certificate in an electronic commerce environment established three roles for the

47. *See* John Gregory, *Authentication of Digital Legal Records*, 6 EDI L. REV. 47 (1999).

48. *See* Jane Kaufman Winn, *Couriers Without Luggage: Negotiable Instruments and Digital Signatures*, 49 S.C. L. REV. 739 (1998) (discussing limitations of procedures used to issue Verisign "Digital IDs").

parties — Certification Authority (CA), Subscriber (S), and Relying Party (RP) — and then tried to map those roles onto recognized business law doctrines.[49] The CA is responsible for issuing certificates to subscribers and for maintaining a list of certificates that have been revoked so that parties who might rely on the certificate can determine whether it is still valid. The S enters into a contractual relationship with the CA, agreeing to submit accurate information when the certificate is issued, to notify the CA if the certificate needs to be revoked, and to take care to maintain control over the private key associated with the certified public key. The RP relies on the digital signature certificate to verify the identity of a subscriber in connection with a particular message that has been signed with S's private key. A prudent RP would never rely on a certificate in any transaction involving substantial risk of loss without first checking the certificate revocation list (CRL) maintained by the CA. This three-sided PKI model corresponds neatly to the telephone directory model: S deals with the publisher of the directory and pays for the listing; once published, the telephone directory is available for any member of the public to use and rely upon in finding phone numbers.

Early adopters of this three-sided PKI model used a certificate practice statement (CPS), which is written by the CA and sets forth the procedures the CA will follow in issuing certificates to establish the rights and obligations of the participants in the PKI.[50] The contract between the CA and S can refer to the standards established by the CPS. For example, the CA may agree to be liable to the S for any losses S incurs with respect to an electronic commercial transaction in which a certificate issued by CA is used to verify S's digital signature, but only if the losses are caused by failure of the CA to comply with the terms of its own CPS. Losses incurred by S for any other reason, including failure by S to retain control over S's private key, would be S's obligations alone.[51]

A major problem with mapping this three-sided PKI model onto a real commercial transaction is the lack of privity of contract between the CA and RP. With regard to a particular electronic commercial transaction, RP is the one trying to manage the risk that S is not actually the person that the

49. This is the model reflected in the ABA DIGITAL SIGNATURE GUIDELINES, *supra* note 18, at 63-90, and has been used by Verisign in distributing "Digital IDs" through its Web site at <http://www.verisign.com>.

50. A complex and technical CPS may be replaced by a simple, more general certificate policy, discussed below.

51. This loss allocation rule is the opposite of the rule currently applied in consumer credit card transactions by Federal Reserve Board Regulation Z, but follows the rule applied for charges for unauthorized use of telephone services. *See* Winn, *supra* note 33, at 1235-37.

signature purports to identify, that S lacks the authority to enter into a binding contract, or that S will be unable to perform his or her obligations under the contract. RP would be willing to pay a third party to help manage those transaction risks, but the three-sided PKI model does not provide a mechanism for RP and CA to bargain for an allocation of that service. Rather, S has the opportunity to review the terms and conditions under which CA issues certificates and determine what level of review by CA for which S is willing to pay. As with the printed telephone directory, S may have a cause of action against CA if the certificate is not issued in accordance with the terms S and CA have set in their contract, but RP is a third party with no rights defined by that S-CA contract, therefore RP has no contractual cause of action against CA.

In the event an electronic commercial transaction goes sour and RP experiences a loss, it would not take long for RP to consider trying to recover from CA if S cannot be found or is judgment proof. One way for CA to manage this risk is to try to establish some basis for a contractual relationship with RP. CA might require RP to agree to be bound by the terms of the CPS and to waive any claims against CA other than those based on CA's failure to follow the terms of its own CPS as a condition of accessing the CRL. Of course, this strategy will only work if RP is sufficiently prudent to check the CRL before relying on it. If RP does not check the CRL before relying, then there would be no obstacle to RP basing its claim against CA strictly in tort.

RP's tort claim against CA would be based on a negligent misrepresentation of information.[52] RP would claim that, notwithstanding the fact that CA may have followed the terms of its own CPS to the letter, the standards established by the CPS were inadequate. As a result, the binding of S to the digital signature certificate gave rise to a reasonable perception by RP that CA had taken reasonable steps to guarantee that S was in fact the person RP believed S to be, when in fact CA had exercised a much lower and negligent level of scrutiny of S's claims before issuing the certificate. Whether or not RP would have any chance of prevailing on this theory would depend on the facts of the case; however, it would seem very likely that RP could withstand any summary judgment motion CA might make, forcing CA to assume very substantial litigation expenses in establishing the validity of its interpretation of the legal rights and obligations created by the three-sided PKI model.

Even if RP clicks on an "I agree" button on the CA's Web site before accessing the CRL indicating agreement to be bound by the terms of the

52. *See* RESTATEMENT (SECOND) OF TORTS § 552 (1965) (defining negligent misrepresentation of information claim).

CPS, it is not clear that this will limit the CA's exposure to litigation with an RP. At best CA can argue that it is granting RP a license to access its database of revoked certificates, and in exchange for the grant of a license, RP must agree to be bound by the terms of that license, including a limit on the contexts under which RP may rely on the binding of S's real world identity to an on-line identity. RP can argue that no contract was formed, because CA received no consideration from RP in exchange for RP being granted access to the CRL if the only thing CA asks of RP is a waiver of RP's right to sue for negligence when CA offers the CRL to the public. CA might be able to bootstrap that limitation of liability for its standard of review in issuing the certificate into a license limiting RP's right to use the data in the CRL, but that is far from a certain outcome. In the three-sided PKI model, CA is clearly conferring some benefit on RP, if RP accesses the CRL, but it is difficult to identify what, if any, benefit RP confers on CA that might count as consideration under classical contract theory. If CA is able to persuade a court that a waiver of negligence claims somehow constitutes consideration sufficient to support a finding that a contract exists between CA and RP, CA has still not cut off all RP's claims to recover its losses in its transaction with S. If the RP is not required to review the terms of the CPS before agreeing, but instead is merely informed that those terms are available for review, the RP may claim that even if a contract is found to exist between CA and RP, the terms of the CPS are not terms in that agreement.

Some of the problems associated with the three-sided PKI model can be ameliorated by making the model four-sided and by introducing the concept of a certificate policy (CP).[53] A CP is a document that may be drawn up by any party, whether a RP or a more general "policy authority" who represents the interests of all PKI stakeholders, stating the minimum standards a digital signature certificate should meet to be acceptable to anyone who has adopted the CP. The three-sided PKI model was designed to serve as a universal open-system PKI that could support commercial or any other transaction in an on-line environment without being tailored to the particular circumstances of the individual transaction. Although the vision of a universal PKI that can work in any on-line environment has largely been abandoned as too ambitious in light of the rudimentary level of develop-

53. *See* National Automated Clearinghouse Association (NACHA), The Internet Council, *Certification Authority Rating & Trust (CARAT) Guidelines: Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates* (last modified Sept. 21, 1998) <http://internetcouncil.nacha.org/CARAT/CARAT921.pdf> [hereinafter *CARAT Guidelines*] (describing implementation of four-sided PKI model with CP); *Federal PKI Task Force Business and Legal Work Group, Model Certificate Policy,* (last modified Mar. 25, 1998) <http://www.mbc.com/model.cp.html> (discussion draft).

ment of the technology and applications of the technology available today, it may eventually prove to be a practical approach to the problem of managing on-line identities. The four-sided PKI model and the development of a CP reflects the efforts by transactors to define the contexts within which digital signature certificate technology will be deployed with greater specificity. As the context within which certificates are better defined, the legal ambiguities of the three-sided PKI model become less intractable.

In a four-sided PKI model, the role of the CA can be split into the roles of local registration agent (LRA) and certificate utility (CU).[54] The LRA is someone who has a pre-existing relationship with S and can therefore provide a meaningful level of scrutiny when certificates are issued to subscribers. The CU provides only the technical services associated with issuing certificates and maintaining a CRL, and has no contractual relationship with either S or RP. The information contained within the CPS in the three-sided PKI model is divided into an internal document stating the technical standards the CU will apply, and a contract governing the relationship between the LRA and S. The contract between the LRA and S may also refer to RP's CP, if S knows it needs a digital signature certificate that will be acceptable to RP. The amount of information S is required to review and agree to in connection with the issuance of the certificate may be less than when the contract between the CA and S incorporates by reference the entire CPS, which is the three-sided PKI model. In the context of a pre-existing relationship between the LRA and S, S has a better chance of understanding the rights and obligations associated with its use of the digital signature certificate. The LRA can also require that S only use the certificates issued by the CU in a particular context and have some confidence that S will honor that limitation. The LRA will require S to limit S's use of the certificate to transactions with only those RPs who agree to be bound by the same terms S has agreed to be bound by in the contract between S and the LRA, and to indemnify the LRA from any use by S inconsistent with the terms of the agreement between S and the LRA. If the LRA has reason to believe that S would not be able to pay for damages S might cause and become liable for under such an indemnity agreement, the LRA can decline to enroll S in the PKI.

If certificates used by RP to verify S's signature conform to the standards stated in the CP and the provisions of the CP correspond to RP's risk management policies, then RP will be relying only on certificates that actually support RP's risk management policies. In order for this to occur, S

54. *See* Alexander Cavalli & Jane K. Winn, *Internet Security in the Electric Utility Industry*, 38 JURIMETRICS J. 459 (1998) (describing LRA's role in a four-sided OASIS PKI model); *see also CARAT Guidelines*, *supra* note 53 (describing a model similar to that used in the OASIS PKI).

must be aware of the provisions of the CP and ask for the LRA to warrant that S's certificate is issued under conditions that meet the requirements set out in the CP. As a practical matter, both the LRA and S will have to understand and accept the terms of the CP. If RP suffers a loss in an electronic commerce transaction and the LRA can show that the loss was not caused by the LRA's failure to observe the standards established in the CP but rather due to some other problem in the transaction, then the LRA will be much more likely to prevail in its efforts to avoid liability on the transaction. This would be true whether RP tried to recover on a tort theory, or on a theory that the terms and conditions that the LRA imposed as a condition to accessing a CRL were not part of a contract binding on RP.

Until the concept of a CP gains wide acceptance in electronic commerce markets, and the terms of CPs are sufficiently standardized to be reflected in standardized notations on the certificates themselves, the benefits of using a CP will be limited. Only a potential S who is engaged in a sufficiently large value or long-term relationship will be able to justify the costs of learning the terms of a CP designated by an RP, and to negotiate with a LRA to guarantee that no certificates are issued to S that do not comply with the CP. While this is not the same as requiring a closed system, it will add considerable cost to transactions executed within the PKI. This may make those transactions more expensive than if they were executed using alternative electronic commerce technologies such as credit card information sent over the Internet using Secured Sockets Layer (SSL) for security.[55]

One suggested solution to the problem of PKI design has been to eliminate the role of the CA altogether and capitalize on pre-existing business relationships for assurance that risk management criteria for transactions are observed even in electronic environments. In the "account authority" model of digital signatures, the public key associated with a particular individual is stored within an existing electronic commerce system.[56] The public key is added to existing account-based information about a transac-

55. In 1999, the standard technology for guaranteeing the confidentiality of credit card information in transit over the Internet is browser-based Secure Sockets Layer (SSL) technology. *See SSL (Secured Sockets Layer)* (last modified Jan. 1, 1999) <http://whatis.com/ssl.htm> (explaining what SSL is and how it works). SSL security is based on a very simple form of PKI. For a general description of the use of SSL and credit cards as a risk management system used in retail Internet commerce, see Jane Kaufman Winn, *Clash of the titans: Regulating the Competition Between Established and Emerging Electronic Payment Systems*, 14 BERK. TECH. L.J. 671 (1999).

56. *See* Anne Wheeler & Lynn Wheeler, *Account Authority Digital Signature Model* (visited Apr. 19, 1999) <http://www.garlic.com/~lynn/aadsover.htm> (explaining how public keys are stored within existing non-face-to-face transaction capability in account authority model).

tor and takes the place of reference to a social security number, mother's maiden name, or last deposit, as an authentication device.[57] The simplicity of the account authority digital signature model reduces the number of obstacles that will have to be overcome before strong authentication technology can be introduced in existing electronic commerce systems such as credit card and debit card transaction systems. From the perspective of transacting parties, the information needed before transactions can be accepted is provided through existing channels in currently recognizable formats, and the authentication technology merely enhances existing network security systems. Before the account authority digital signature model can actually be implemented, however, changes in existing standards for electronic financial transactions will have to be revised, and existing applications based on those standards will have to be upgraded. In 1999, it was still unclear whether such streamlined applications of asymmetric cryptography would gain widespread acceptance in the electronic commerce market.

Participants in a limited number of pilot projects based on the use of PKIs to facilitate commercial transactions in on-line environments have made their findings public. These include the Securities Industry Root Certification Authority (SIRCA)[58] and the Certification Authority Interoperability Pilot of the Internet Council of the National Automated Clearing House Association (NACHA).[59] In terms of the contrast developed above between the three-party and four-party models, the SIRCA pilot used the four-party model because each securities firm acted as an LRA for its individual employees.[60] The NACHA pilot used the three-party model, permitting individuals to select a CA and have a certificate issued without the intervention of an LRA for the purposes of the pilot.[61] In view of the lack of any substantive screening of individual participants, the certificates issued contained no information that linked the certificate to a real world person, but rather referenced a dummy account number that had been

57. *See id.* (describing how public keys in account authority model replace existing authentication devices).

58. *See Securities Industry Root Certificate Authority (SIRCA) Concept Paper* (last modified Apr. 26, 1998) <http://www.sia.com/sirca/> [hereinafter *SIRCA Concept Paper*] (explaining function of SIRCA).

59. *See* David Merrit & Juan Rodriguez Torrent, *Building an Environment of Trust: Certificate of Authority (CA) Interoperability* (last modified Aug. 3, 1998) <http://www.usenix.org/events/cc98/pki/torrent_html/index.htm> (describing NACHA's PKI pilot project).

60. *See SIRCA Concept Paper*, *supra* note 58 (explaining how each SIRCA pilot securities firm functions as an LRA).

61. *See* Merrit, *supra* note 59 (describing how NACHA pilot customers can choose participating financial institution as CA).

established for the pilot.[62] Following the completion of the first NACHA pilot in 1998, a second pilot project is underway in 1999 that will test a wider range of payment functions.[63] The second pilot, however, may still involve pseudonymous certificates, dummy account numbers, and simulated transactions, since the focus of the pilot is not transaction risk management, but the possibility of integrating browser-based user interfaces into existing payment systems. Neither of these pilot projects involved the execution of real transactions on-line in reliance on digital signatures, but instead were designed to permit pilot participants to familiarize themselves with the use of the technology. Outside these pilot projects, a large number of organizations have adopted PKIs to enhance security of their internal operations. While these organizations may be conducting tests with trading partners involving the execution of real transactions on-line in reliance on digital signatures, the results of such tests are not generally made available to the public.

V. TRUST MANAGEMENT VS. RISK MANAGEMENT

With regard to information system security, systems can be evaluated in terms of their trustworthiness. Management of the trustworthiness of an information system includes managing the ability of the information system to resist known threats and to perform reliably under a wide range of foreseeable adverse circumstances.[64] This sense of the word trust greatly differs from the legal sense of the word, it also differs from the business practice of risk management. Risk management in a business context generally involves pooling risks to make them more predictable and hedging identified risks by matching them where possible with assets or liabilities to offsetting risk characteristics.[65]

Information systems cannot be proven to be "secure." Information systems can be designed according to the best available system security principles, but because existing systems may have weaknesses which can be exploited to breach current security features, it is not possible for any operating system to prove that it meets some absolute standard of security. As a result, the system security managers aim for a standard of "trustworthiness," which conveys the thought that the system has been tested against all

62. *See id.*

63. *See id.*

64. *See* SCHNEIDER, *supra* note 34, at 2 (explaining importance of trustworthiness to network information systems).

65. *See* FRANK J. FABOZZI & ATSUO KONISHI, THE HANDBOOK OF ASSET/LIABILITY MANAGEMENT: STATE-OF-THE-ART INVESTMENT STRATEGIES, RISK CONTROLS AND REGULATORY REQUIREMENTS (1996) (discussing pooling and hedging against risk in a business context).

known threats, and within the constraints of available resources can withstand them. The concept of trustworthiness is not limited to internal computer processes or the design of network communications, but includes the security of the physical equipment as well. The notion of trustworthiness conveys the idea that for any given input, the information system can be trusted to generate a specific output because its processes are as resistant as possible to corruption from internal or external forces. Any information system must be reliable to a degree, but the label "trustworthy" is reserved for information systems that have been evaluated and tested with regard to their ability to withstand known security threats, which is a characteristic of very few computer systems used for processes requiring heightened levels of security. This notion of trustworthy information systems was originally developed within the military. As more businesses move the management of valuable assets and processes on-line, more businesses require access to information systems providing a level of security similar to the trustworthy systems developed by the military, either under their own control or by agreement with operators of such systems.

The legal definition of trust includes the notion of performance that conforms with certain standards, but unlike the concept of a trustworthy information processing system, recognizes that an element of discretion on the part of the trustee may be unavoidable. The feudal origins of the Anglo-American doctrine of trust involved making a transfer of rights in real property that was absolute on its face but intended by the parties to be less than a complete grant of ownership rights because the nominal owner was expected to maintain the property for the benefit of another.[66] The legal concept of trust is thus based on a general concept of fiduciary duty, which includes predicting what the trustee will do only in very general terms while permitting the trustee discretion to make specific decisions as problems arise that the grantor could not foresee. Trustworthy information systems, unlike trustees, are not expected to evaluate new contexts in light of general standards but are expected to execute specific functions with the highest degree of reliability possible. The Anglo-American legal concept of trust must therefore clearly be distinguished from the technological standard of trustworthy.

Risk management involves loss avoidance, loss pooling, and hedging. Loss avoidance involves adapting business processes to reduce the aggregate level of losses associated with specific operations, and is similar to the

66. Fiduciary obligations not recognized by the common law writ system were nevertheless given legal effect by the Chancery exercising its jurisdiction as a court of equity from its earliest operation. The English law of trusts was more fully developed following the enactment of the Statute of Uses in 1536. *See generally* CHARLES DONAHUE ET AL., CASES AND MATERIALS ON PROPERTY 348-53 (3d ed. 1993).

information system security concept of trustworthiness. Loss pooling involves tolerating a given level of statistically predictable losses and setting aside financial resources to compensate for those losses when they occur. Future losses can be estimated based on models derived from historical experience applied to the best information available about likely future developments. Where hedging or insurance is possible, businesses will face a choice of how much risk to assume, and how much to pay to offset risk or shift it to another party.

In a business management context, decision makers will face choices about declining business likely to come with too high a risk of loss, or accepting business but paying a price in diminished profitability through hedging or insurance costs. For example, a business making the decision to do business on-line will have a choice between making its own decisions about which orders to accept and which to decline, and paying for sophisticated software that can assist the merchant in making those decisions.[67] In making the decision to buy the software, the manager will have to evaluate not just the purchase price of the software but also the cost of running it on existing information systems, or if that is not possible, the cost of upgrading an information system, the cost of training staff to insure the necessary information is run through the software and can interpret its findings, the cost of business lost through possible false positives indicating a high risk of fraud or error when none is in fact present, and a range of other costs. If the software is expensive to purchase or operate, a business may not be able to justify purchasing it if the cost exceeds its predicted fraud and error losses operating without it. The design of business information systems specifically incorporates this type of tradeoff, but the design of those systems designated "trustworthy" does not do so, or at least not to the same degree. In the historical context of Cold War military information system security where the term "trustworthy" was first used, there were few practical constraints on the volume of resources that could be invested to achieve the desired result, and trustworthy information systems were supposed to be as safe as it was possible to make them.

When business information systems were based on centralized, mainframe computer systems, there were reasonably well-established standards for policing system security. The design of secure information systems has become considerably more complex with the advent of client/server computer systems, the Internet, and the practice of mixing and matching various "off-the-shelf" software packages within systems.[68] Security has not

67 Such software can evaluate credit card orders as received and rate those orders in light of historical experience with regard to the likelihood that the information in the order is fraudulent, or contains errors that will cause the merchant to suffer losses.

68. *See* SCHNEIDER, *supra* note 34, at 12-23 (discussing growth and dependence on

kept pace with innovation in the business use of computers, and as a result, client/server networked information systems in general do not possess the same level of security as the old, centralized mainframe systems. There is now a growing recognition that information system security is one of the operational variables that must be taken into account in risk management.[69] As a result, the tradeoffs between greater security and resistance to known threats will have to be balanced explicitly against other business objectives such as speed of transaction processing, ease of the use of computer facilities, decentralized exercise of discretion by users, geographic dispersion of access, and other factors. With this integration of information system security factors into the general business calculus of risk management, the notion of trustworthiness of information systems may depart from the historical meaning of categorically as resistant to threats as is possible to build, and take on a meaning closer to incorporating an appropriate level of resistance to threats in light of the business context and level of resources available for all objectives including security.

VI. SHOULD EITHER HEDGEHOGS OR FOXES ACCEPT DIGITAL SIGNATURES?

Public key infrastructure design to date would seem adequate to support the type of risk management typical of the public sector, although it is clearly not yet sufficiently nuanced to support private sector risk management.[70] The notion of a trustworthy system was developed within the public sector without reference to the kind of cost/benefit balancing that cannot be avoided within private sector risk management contexts. Until more advanced technologies, such as the use of standard certificate extensions to refer to certificate policies in certificates can be standardized and become widely used, digital signature certificates can only provide a snapshot of a limited number of variables at a specific point in time.[71] One of the most common variables a digital signature certificate is used to represent is the identity of a human actor, which is too gross a concept to support most business transaction applications. Risk management that takes transaction level risks as a basic input will not be compatible with the use of a PKI until better ways are found to either integrate PKIs with existing business in-

---

network information systems and vulnerabilities which are included creating need for more complex systems).

69. *See, e.g.*, Ernst & Young, *Assurance and Advisory Service with an Eye to the Future* (visited Apr. 19, 1999) <http://www.ey.com/aabs/> (presenting information systems security background and business).

70. *See* Gregory, *supra* note 47, at 58.

71. *See* FORD & BAUM, *supra* note 38, at 226 (describing current limitations of digital signature certificates).

formation systems, as in the AADS model, or modify the structure of the PKI permit the processing of more transaction-specific information. Simply knowing the identity of a party or having a snapshot of an individual's creditworthiness at an earlier point in time is not adequate to support a decision to execute or decline to execute a transaction at a later date.[72] Current automated business transaction systems have a variety of processes that channel the flow of necessary information to decision-makers, such as on-line authorization systems that provide up-to-date information about a counter-party's creditworthiness. The work of integrating the technology that provides such information to decision-makers and the technology that provides a PKI has not yet advanced beyond the level of pilot projects.

Simple identity might be suitable as an analog to citizenship in the public sphere, where liberal notions such as equality before the law are meant to diminish the significance of variations between individual identities under certain circumstances. As a result, it might seem reasonable to conclude the current design of PKIs seem well suited to the needs of public sector hedgehogs while poorly suited to the needs of private sector foxes. Risk management is only one of many factors that go into the articulation and realization of the public interest, however. Before suggesting that the public sector should invest in developing a PKI to support on-line civic interactions, at least two issues need to be addressed: first, whether there is any public interest in using this technology in light of the potential for adverse consequences its use may have; and second, whether there is any justification for using the sovereign immunity risk management model even when this technology is being used by the government or for a public purpose.

One of the most obvious reasons a democratic government might be interested in the use of on-line communications would be a desire to enrich and invigorate public discourse. There is a conflict, however, between the manner in which a PKI supports more secure communications in an on-line environment and the values of vigorous public debate. The ability of computers to capture and store information that associates particular individuals with on-line activity, including on-line speech and on-line accessing of information, raises profoundly troubling issues of how classical liberal values can be preserved in on-line environments.[73] These are issues about which

72. Peter Freund, Chairman of CertCo, Inc., pointed this out to me.

73. *See, e.g.*, Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1003-19 (1996) (advocating that First Amendment rights to read anonymously applies in cyberspace); A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 479-82 (1996) (expressing concern over possible erosion of privacy on Internet); Lawrence Lessig, *Constitution and Code*, 27 CUMB. L. REV.

the public debate in the United States has barely begun, and with regard to which no consensus yet exists.

In 1998, the U.S. General Services Administration launched an ambitious project to provide more government services on-line. This project included Access Certificates for Electronic Services (ACES),[74] a PKI to provide identity-based authentication where necessary in on-line interactions between members of the public and the federal government. This program immediately raised concerns among privacy advocates. The Center for Democracy and Technology described its concerns in the following terms:

The ACES project threatens individual liberty and privacy by:

- escalating the collection and centralization of data about an individual's identity and activities, potentially increasing government intervention in our daily lives. The registration authorities must be multiple, diverse and, where possible, created only for programmatic purposes. ACES' current plans to have a few large registration authorities with similar core elements would, in practice, not meet this goal.
- creating a de facto identity requirement for every interaction with the government. The project should strive to aid in the limitation of the collection of personal information online. Simply mandating agencies to allow all services off-line, avoids dealing with the difficult concerns around these issues.
- failing to establish fair information practices to protect data collected and generated by its use.[75]

Until some form of consensus emerges on these difficult issues, it will be difficult to articulate standards regarding the proper use of this technology by government.

Even if the public benefit derived from adapting a PKI to use in the public sector can be clearly established, it remains unclear whether there is any justification for applying a sovereign immunity risk management model to that use. The sovereign immunity risk management model authorizes the shifting of risks either away from parties providing infrastructure services, such as certification authorities, onto parties using the PKI, or away from parties who wish to rely on a digitally signed message onto parties whose digital signature may have been affixed without authorization. The most

---

1, 7 (1996) (posing questions of Fourth Amendment protection in cyberspace).

74. *See Access Certificates for Electronic Services* (visited Apr. 19, 1999) <http://www.gsa.gov/aces/> (detailing information about ACES project).

75. *See Response To Letter From General Services Administration (GSA) Addressing CDT's Concern On the Access Certificates For Electronic Services (ACES) Initiative* (June 29, 1998) <http://www.cdt.org/digsig/gsaletterrep.html> (arguing successful implementation of ACES project would undermine both individual privacy and healthy development of Internet).

traditional justification for sovereign immunity, that the king cannot be haled into his own courts without his permission, can no longer plausibly be used to justify such shifting of risks away from the public sector party to a private sector party. It is also unclear, however, whether the more modern justification for sovereign immunity is valid in this case. That justification permits externalizing risks away from public sector actors onto private sector individuals in order to prevent the public sector actors from becoming hobbled by the threat of potentially crippling liabilities. If more sophisticated risk management strategies are being developed in the private sector, and those strategies can be adapted for public sector use, then the apparent conflict between imposition of liability and accomplishment of public purpose might be eliminated.

Licensing statutes, such as that adopted by Utah, provide a clear shelter from liability for CAs that meet rigorous licensing standards.[76] As a regulated entity, the CA would enjoy the same kind of immunity from liability the state itself enjoys provided it operates within the framework established by the Utah statute.[77] This limit of liability is premised on the assumption that the licensing framework established by the statute will minimize or eliminate the most serious risks to the public associated with the use of digital signatures and create the electronic equivalent of a regulated financial institution or a common carrier. If the licensing framework fails to create the functional equivalent of an on-line common carrier, then the statute will have authorized a transfer of resources from users of the technology to the owners of the infrastructure services without having guaranteed public benefit in return. Until there is some experience regarding how infrastructure services are in fact used, it will be impossible to determine whether the licensing statutes have achieved their objective.

Statutes that shift the risks of unauthorized use of digital signatures away from the parties relying on those signatures to the parties whose signature was used without authorization create a subsidy for relying parties at the expense of subscribers.[78] If the same parties are both relying parties and subscribers, then there would be no distributional effect from this shift in liabilities. If, however, some parties are consistently relying parties, and others are consistently subscribers, then there will be a shift in costs from the first group to the second. If the first group are merchants who deal directly with developers of on-line authentication technology, and the second group are consumers who make purchases of mass market off-the-shelf software and hardware with limited abilities to evaluate the functionality of

76. Utah Digital Signature Act, UTAH CODE ANN. § 46-3-101 (1998).

77. *See id.* § 46-3-309 (granting licensed CAs limited immunity from liablity).

78. *See* C. Bradford Biddle, *Legislating Market Winners* (1997) <http://www.w3journal.com/7/53biddle.wrap.htm>.

the technology or to have input into its design, then such a shift will actually undermine existing incentives for developers of infrastructure technologies and their primary customers, the on-line merchants, to improve the functionality of these technologies.

There may be a basic misconception about how new technologies such as PKIs will map onto social institutions built into law reforms aimed at aiding technology developers, service providers, or relying parties such as merchants. This misconception has been called "cyberspace utopianism"[79] or "cyberanarchy."[80] The misconception consists of presuming that conditions in cyberspace are so different from those prevailing in other environments regulated by modern legal orders that wholly new responses must be devised in order to permit orderly social interactions to take place. If on-line authentication services are so novel and so unrelated to existing systems for identifying counter-parties that prior precedents cannot be helpful, and there is some kind of moral imperative for governments to move quickly to enshrine recognition of that novelty in statutory liability regimes, then either the licensing model or the relying party protection model of risk shifting are justified by sound public policy. This cyber-utopian vision about the supposed novelty of on-line social interactions resonates with the hedgehog's totalizing vision, and the philosophical visions of some of the noted hedgehogs in history such as Marx, Rousseau or Plato.

On-line authentication services may in fact be dramatically more difficult to accomplish in a "cyberspace" world in which strangers collide in a social vacuum, divorced from all prior contexts and relationships. If such a "no prior relationship" transaction is the one that on-line authentication methods must be designed to solve, then perhaps a legislative subsidy in the form of limited liability for the developers and providers of this service can be justified. There is already evidence, however, that the most successful examples of "cyberspace" commerce to date are not based on terribly novel models after all. Some of the most successful Internet businesses actually conform closely to established models of electronic commerce, such as electronic verification and processing of credit card charges, or electronic data interchange contracting.[81] If incremental changes in elec-

79. John Rothchild, *Protecting the Digital Consumer: The Limits of Cyberspace Utopianism*, 74 IND. L.J. (forthcoming 1999).

80. Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998) (arguing cyberspace transactions are no less resistant to conflict of law issues than other non-cyberspace transactions).

81. Among the most successful Internet electronic commerce merchants are Cisco Systems Inc, which is using a modified EDI model to make more than $1 billion in sales per quarter, see *Cisco Connection Online The Worldwide Leader in Networking for the Internet* (visited Apr. 19, 1999) <http://www.cisco.com/>, and Dell Computers, which is using credit cards to make more than $14 million in sales per day over its Web site, see *Dell Computer*

tronic commerce models developed for an earlier generation of networked computer systems can meet the needs of most parties wishing to interact in cyberspace, then there is no compelling public need at this time to subsidize the development of solutions that support anonymous interactions between strangers in "cyberspace." This older generation of standards for electronic communications resembles the empirically-based, detail-oriented vision of the fox. While the fox's narrower, more focused vision lacks the charismatic appeal of the hedgehog's sweeping vision, it may provide a firmer foundation for articulating public policy in this area.

CONCLUSION

Berlin studied Tolstoy's philosophical discourses embedded within *War and Peace* and found that, notwithstanding his aspiration to a hedgehog-like encompassing vision of the human condition, Tolstoy could not avoid, fox-like, being distracted by its complexity and ambiguity.[82] This study of the early stages of designing and implementing PKIs to enhance the security of open public networks such as the Internet has come to a similar conclusion. While many sincere believers in the importance of this new technology have advocated hedgehog-like liability limits for those promoting its use in both public and private sector applications, careful analysis reveals that fox-like risk management strategies are more likely to be appropriate for private sector applications. Furthermore, risk management strategies developed for private sector transactions might find applications in public sector uses for this technology, and might eliminate the need for law reform to change current liability rules. The risk management strategies appropriate to public and private sector applications of this technology may ultimately diverge; at this time, however, both public and private sector risk management strategies are still under development. Until the form of those strategies has more clearly taken shape, there is good reason to hesitate before locking in mandatory loss-shifting regimes through legislation even for public sector uses.

The technological infrastructure to support secure electronic commerce conducted over open networks such as the Internet is being put in place today. The appropriate legislative response to those developments is unclear, and different governments are trying a wide range of approaches. Which business models will permit parties to capitalize successfully on these developments is likewise unclear, and a bewildering array of enterprises are competing to establish standards in this area. The government, acting to

---

First Major PC Company to Offer Protection Against Credit Card Fraud with Secured Shopping Guarantee (last modified Sept. 18, 1998) <http://www.dell.com/corporate/media/newsreleases/98/9808/13.htm>.

82. *See* HEDGEHOG & FOX, *supra* note 1, at 80.

advance the public interest, must look at these developments as a whole and evaluate their relationship to established social and political policies. The globalizing perspective of the hedgehog, combined with its impenetrable defenses against attack, is appropriate when the whole is visible, which is arguably not yet the case.