6-1999

Considerations for an Effective Telecommunications-Use Policy

Michael E. Whitman
Kennesaw State University, mwhitman@kennesaw.edu

Anthony M. Townsend
University of Delaware

Robert J. Aalberts
University of Nevada, Las Vegas

Recommended Citation

Whitman, Michael E., Anthony M. Townsend, and Robert J. Aalberts. "Considerations for an Effective Telecommunications-Use Policy." Communications of the ACM 42.6 (1999): 101-108.

Michael E. Whitman,
Anthony M. Townsend,
and Robert J. Aalberts

Considerations for an Effective Telecommunications-Use Policy

Creating effective use through effective policy.

Recent changes in federal telecommunications legislation have underscored the importance of an up-to-date and effective telecommunications-use policy in business organizations. With the proliferation of the Internet, intranets, and email as commonplace business tools, the potential for misuse and subsequent liability has become an increasing concern. Even though the recent Supreme Court decision[1] struck down the obscenity provisions of the Communications Decency Act (CDA)[2], it left intact legislation that effectively mandates development of a sound telecommunications-use policy. In addition to potential liability for systems misuse, organizations have also had to address issues of individual employee privacy within the new systems [5].

This technical expansion, coupled with the information privacy issues, has created a large gray area in organizational policy-making. What exactly should an organization formalize as a standing operational policy for day-to-day use of its telecommunications systems? As is evident, without a specific policy that addresses systems use, there can be no expectation of ethical and responsible use on the part of either an organization or an individual employee.

A sound telecommunications policy serves a variety of purposes within an organization. First, it codifies system controls and reporting authorities. Second, it reinforces the organization's expectations about how telecommunications systems should be used. Third, it serves to indemnify the organization against liability for an employee's inappropriate or illegal system use. A published telecommunications policy serves as a legally binding agreement between parties (the organization and its employees) and shows that the organization has made a good

[1] Reno v. American Civil Liberties Union, No. 96-511 (June 26, 1997).
[2] Title 47 U.S.C.A 223 et seq.

faith effort to ensure that its telecommunications systems are not used in an illegal manner.

In spite of the apparent need for sound telecommunications-use guidelines, formal policies are far less common than one would think. Even rarer are published policies demonstrating willingness to balance the needs of users with the security needs of the organization. To address the challenge of effective policy development, this article seeks to thoroughly examine a large sample of existing organizational policies and then elaborate a standardized format for the internal development of an effective telecommunications-use policy. Although the development of a telecommunications-use policy is highly dependent on the technologies and context of each organization, there are several aspects of policy development common to most organizations.

Table 1. Fair and responsible use of telecommunications technology.

I. Statement of Policy
- Scope and Applicability
- Definition of Technology Addressed
- Responsibilities

II. Authorize Access and Usage of Equipment
- User Access
- Fair and Responsible Use
- Protection of Privacy

III. Prohibited Usage of Equipment
- Disruptive Use or Misuse
- Criminal Use
- Offensive or Harassing Materials
- Copyrighted, Licensed or Other Intellectual Property
- Other Restrictions

III. Systems Management
- Management of Stored Materials
- Employer Monitoring
- Virus Protection
- Physical Security
- Encryption

V. Violations of Policy
- Procedures for Reporting Violations
- Penalties for Violations

VI. Policy Review and Modification

Scheduled Review of Policy and Procedures for Modification

VII. Limitations of Liability

Statements of Liability or Disclaimers

Previous Policy Research

There are a number of studies [4, 7, 8, 10] that call for the implementation of policies to govern the use of computer and telecommunications resources. There are, however, a number of studies that address the development of more general computer-use policies that provide some framework for the development of sound telecommunications policy.

Bergeron and Bérubé [2] propose three guidelines for the formulation of computer policies, which can be applied to telecommunications policy development. First, all policies must contribute to the growth of the organization. Second, management must ensure the adequate sharing of responsibility for computer systems use. Finally, end users should be involved in policy formulation. The authors further note that while policies should be complete and comprehensive, too many policies or policies that are too complex could lower end user satisfaction.

Existing research on computer-use policy has tended to focus on security issues associated with computer systems, including the security of the telecommunications component of the system [12]. Lindup [4] stipulates that any information security policy should address systems security, product security, community security and corporate information security. Scoma [6] stresses that any security posture (subsumed in a general telecommunications-use policy) also should address managerial oversight, periodic checks, establishment of clear policies and self-audit and control functions in each department.

Study Format

The present study's research methodology consisted of a three-part process. First, the study sought to identify a broad range of policy components that address telecommunications issues. Second, it sought to determine the extent to which current organizational policies include the full range of telecommunications components. Finally, it evaluates this policy framework from a legal perspective to ensure that it provides the basis of a fully compliant telecommunications policy.

A total of 90 policies that addressed a spectrum of information technology issues were collected and reviewed. These included policies from 26 businesses[3], 25 government and nonprofit organizations, and 39 academic institutions. These documents were reviewed to determine the range of policy components among extant policies; not all contained all

[3] A total of 55 businesses were actually contacted and asked for any computer or telecommunications-use policies. Of these, only 26 had some form of policy. This is significantly fewer than the 83% reporting a computer-use policy and the 87% reporting a communications use policy in the WarRoom, 1996 [12] study. The WarRoom study had a 41% usable response rate; it is possible that firms without policies did not respond proportionally.

components. These elements formed the framework (see Table 1), against which each policy was reviewed and coded as to its structural componentry (for example, does the policy address criminal use of the system and does it address fair and responsible use?). Table 2 presents each major potential policy component, along with the percentage of commercial, organizational, and educational policies that addressed it. Of the 90 policies reviewed, fewer than 5% addressed every telecommunications issue contained in the overall framework; the remainder only partially addressed the full range of telecommunications issues identified. Overall, 49% of policies contained language that fully defined authorized access and use of equipment, 18% had language fully addressing prohibited usage of equipment, and less than 1% had language fully addressing proper systems management.

Table 2. Analysis of framework components in studied policies.

	COM	GOV	EDU	ALL
	In Percent			
I. Statement of Policy				
Scope and Applicability	34.6	68.0	66.7	29.8
Definition of Technologies				
PC/LAN	61.5	80.0	97.4	42.4
WAN/Internet	42.3	88.0	92.3	39.6
Email	50.0	52.0	69.2	30.4
Fax/Image	7.7	0.0	2.6	1.7
Phone/Vmail/Cellular and Pager	38.5	16.0	5.1	9.2
Responsibilities	50.0	76.0	71.8	34.4
II. Authorized Access and Usage of Equipment				
User Access	61.5	96.0	97.4	44.7
Fair and Responsible Use Criteria	73.1	76.0	76.9	39.0
Protection of Privacy	38.5	56.0	74.4	30.4
III. Prohibited Usage of Equipment				
Disruptive Use or Misuse of Equipment	42.3	84.0	94.9	39.6
Criminal Use	23.1	68.0	79.5	30.9
Offensive/Harassing materials	38.5	44.0	61.5	25.8
Copyrighted/Licensed or other Intellectual Property	61.5	76.0	87.2	39.6
Sensitivity and Control of Company Materials	57.7	52.0	38.5	24.7
Other Restricted Materials	65.4	36.0	33.3	22.4
IV. Systems Management				
Management of Stored Materials	30.8	56.0	48.7	23.5
Employer Monitoring	38.5	28.0	41.0	18.9
Virus Protection Requirements	26.9	44.0	12.8	13.2
Physical Security Requirements	30.8	24.0	20.5	12.6
Encryption Requirements	11.5	12.0	10.3	5.7
V. Violations of Policy				
Procedures for Reporting Violations	15.4	20.0	17.9	9.2
Penalties for Violations	57.7	44.0	71.8	3.1
VI. Policy Review and Change				
Scheduled Review of Policy and Procedures	7.7	8.0	15.4	5.7
VII. Limitations of Liability				
Statements of Liability or Disclaimer	19.2	24.0	7.7	8.1
n=	26	25	39	90

Telecommunications Policy Framework

Most policies begin with an introduction of the fundamental philosophy of the organization with regard to the topic at hand. Policies focusing on telecommunication technology should begin in this manner, assuring the employee that the overall premise for having such a policy is not to provide a legal foundation for persecution or prosecution. It is designed to provide a common basis of understanding of exactly what the employee can and cannot use the technology for. Once the gray area is removed, the employee is free to use the technology, without having to constantly ask, "May I do this?" This serves to protect both the employee and the organization from potentially difficult circumstances.

We will now lay out the framework of a comprehensive telecommunications policy, organized by section and subsection numbers. For each section or subsection, we describe the purpose of the section, and where applicable, discuss relevant law that mandates the section.

Statement of policy. The first section defines the scope and applicability of the policy, the technologies covered and their accompanying definitions, and the expected responsibilities of individuals affected by the policy.

Scope and applicability. By explaining the purpose of the policy, the employer lays the foundation for the rest of the document. The reason for the policy should be clearly articulated, so that the employee can understand the intent of the material. Once this purpose has been established, the document must clearly identify who is covered by the policy, in terms sufficiently specific to preclude any misunderstanding.

Definition of technology addressed. This next section should define exactly which telecommunications technologies are covered under the policy. This will of course depend on what capabilities the organization currently employs, but can be expanded to include the future adoption of known technologies. This will permit continued use of the policy with only minor changes. Currently, the policy should be written to at least include all of the technologies described in 47 U.S.C. 153, which defines systems currently subject to federal regulation. Generally speaking, this includes any device capable of transmitting or receiving information across a state boundary. Thus virtually any device that operates through phone lines or external data links is included.

THE OVERALL PREMISE FOR HAVING SUCH A POLICY IS TO PROVIDE A COMMON BASIS OF UNDERSTANDING OF EXACTLY WHAT THE EMPLOYEE CAN AND CANNOT USE THE TECHNOLOGY FOR.

Responsibilities. The responsibilities of each individual covered in the policy should be defined to permit effective use of the technology. Users should be tasked to use the system in the manner for which it was intended, and to consult the policy contact persons if any questions arise. Managers and IS personnel also receive special tasking, to the extent to which they are responsible for ensuring that end users comply with the policy.

Authorized access and usage of equipment. The second major policy section generally defines permissible uses of the telecommunications systems. The purpose of this section is to clearly describe who may use the telecommunications system and how permitted users may correctly use the system.

User access. Here, the policy defines the various categories of employees who are permitted access to telecommunications technology and the extent to which access is provided. The level of access, or what may be accessed, can range from LANs, to external networks or the Internet. Any relevant time restrictions on period and duration of use are outlined as well (for example, employees can only use the Internet during personal breaks).

Organizational policy should address a number of issues relevant to the management of access to these systems. Format of passwords and usernames must be structured yet manageable. Additionally, in the event of dismissal or termination of employees, how access is revoked and how security procedures are implemented must be addressed.

Fair and responsible use. Generally speaking, an employee is empowered to use technology provided by the employer for the purpose of conducting the employee's regular business activities, although the employer may extend this definition to various levels of authorized personal use. This typically falls into four levels of permissible systems use: 1) Restricted to business use only; 2) Authorized emergency personal use; 3) Authorized occasional personal use; 4) Unrestricted personal use, depending on the needs of the organization.

Protection of privacy. The protection of privacy is of concern to employees, organizations, and their clientele. This concern for privacy differs according to perspective: at the individual level, employees want to know that their private communications remain private. At the organizational level, there is a desire to provide employees with sufficient privacy to demonstrate organizational trust and to allow them effectively to conduct the organization's business, while at the same time maintaining enough monitoring of employee system use to prevent illegal or inappropriate behavior. Privacy expectations will vary from one firm to the next; what is critical in this section of the policy is that individual privacy rights be clearly articulated.

[4] Traditionally, the concept of privacy applies to individuals; frequently, however, the relationship between organizations and their clientele is of a sufficiently confidential nature that privacy rights may apply [9].

Privacy of communication between the organization and its clientele[4] must also be addressed in this section of the policy. Attorney/client interactions, proprietary information, and other intellectual property frequently move through telecommunications systems. The telecommunications policy must clearly articulate that such private information will be inviolable. Employers may even wish to include a "Trade Secret/Confidential Information Covenant" in their employees' employment contract as well. By including clear language addressing the privacy of clients' information, the policy reassures clients that their information is secure, as well as delineating individual employee responsibility for information privacy.

An employee's rights to privacy are defined by the U.S. Constitution, state constitutions, both state and federal statutory law, and the common and statutory law of the various states. Voice and email communications are included as potentially protected by rights of privacy under the Fourth Amendment for government employees at the federal, state, and local levels. Privacy rights of employees in the private sector are not protected unless they are afforded such protections under state or local laws. Privacy rights for employees must be clearly articulated in this section; without clear guidelines, courts may construct privacy rights based upon employees' subjective or objective expectations.

Prohibited usage of equipment. Perhaps the most sensitive area for employers and employees alike is the restriction as to how employees may or may not use organizational equipment both during performance of their work and for any personal activities. This section defines a range of impermissible systems usage.

Disruptive use or misuse. This subsection addresses any use of the system that could result in interference with the work of others, unauthorized deletion or modification of others' files, overuse of the system and the systems resources, or generally any use that could be interpreted as computer waste or abuse. These prohibitions must be designed to fit the company's culture and work context, to prevent the creation of a policy that over- or understates the particular restrictions on system use.

Criminal use. Any policy addressing the use of a system should contain a strong statement condemning the use of that system for any illicit or criminal activity. In telecommunications systems this also specifically includes the use of the system to access or attempt to access this system or any other systems without proper authorization, as well as attempts to access unauthorized areas of the system itself (for example, email files). It should also include use of the system to develop or implement any virus-type program, or generally in any activity that could be construed as legally questionable. While this certainly prohibits illegal system use, the following sections more clearly articulate specifically prohibited illegal system use. Inclusion of these sections is critical; their specificity helps demonstrate a good faith effort on the part of the organization to prevent illegal system use.

Offensive or harassing materials. For electronic media, the Communications Decency Act of the Telecommunications Act of 1996 specifically prohibits the presentation or transmission of sexually harassing or offensive material over telecommunications devices. These restrictions should also be required to protect against hostile environment claims under sexual harassment statutes, as there have been a number of cases involving employer liability for the transmission of offensive and harassing materials.

Several employers have been the targets of lawsuits involving sexually explicit material on the Net. For example, Chevron Corporation paid a $2.2 million settlement to four women, paid over $1 million for the women's attorneys' fees, endured 2-1/2 years of discovery and a great deal of negative media attention, in a sex discrimination suit based partly on sexually harassing email messages [1].

Harassment, to be actionable under antidiscrimination laws, does not have to be sexual in nature. Email can be used to support allegations of harassment based on race, age, disability, national origin and other protected classifications. For example, in *Gibson v. American Library Association*[5], email received by the plaintiff was used to support his claim of racial harassment. Thus the prohibition against using the telecommunications system to transmit or receive harassing messages indemnifies the employer against a variety of potential actions.

Copyrighted, licensed or other intellectual property. There is clearly defined legislation in place that regulates the storage, duplication and transmission of copyrighted material, including software, printed materials, and other intellectual property. When the company's computer system can allow users to transmit or receive copyrighted materials, such as through a LAN or the Internet, the telecommunications policy must include a statement requiring complete compliance by users to all intellectual property laws. The policy should also detail all relevant regulations, as well as the employees' responsibilities within them.

Sensitive company materials. It is essential that organizations establish positive control of the confidential-

[5] 846 F. Supp. 1330 (N.D. Ill. 1993).

ity and security of sensitive company materials, that are accessible through a telecommunications link. The policy should detail a system for classifying the sensitivity of various types of information, and should detail the mechanism for its control and distribution. A four-category example of such a classification scheme might include (1) publicly available information; (2) internal or official use information; (3) confidential, sensitive, or restricted information; and (4) highly restricted or highly sensitive information. Clearly labeling all correspondence and specifying in the policy who has authorized access to each level of information can obviate unauthorized dissemination.

Other restricted materials. Organizations may also choose to restrict use of the telecommunications system for the transmittal of advertisements, or other nonorganizational commercial use, including political and charitable solicitations, and personal advertising.

Systems management. This section describes the employer's scheduled management of the telecommunications system(s) including when, where, and how stored materials will be archived or removed. In this capacity, it also addresses the extent to which materials such as personal documents, email and voice mail messages may be subject to employer review. The section also contains policy directing employee responsibilities to protect archived materials and current systems from external threats.

Management of stored materials. Many telecommunications technologies have the capability to store and retrieve past messages in various forms. Email and voice-mail in particular have specific database storage areas on a central server, independent of the terminal device used by the employee. For systems capable of storing messages, the finite amount of storage space eventually becomes congested. When this occurs, the messages must be voluntarily or involuntarily purged from the system. The policy must clearly specify how, when, and by whom these messages are to be removed. The policy should also detail how and when users will be notified of potential system purges, and should specify a time frame and procedure for users to relocate critical documents. Voice-mail systems, unlike traditional analog answering services, suffer the same storage constraints, and therefore should be managed similarly.

Employer monitoring. Another area of intense legal scrutiny is employer monitoring of employee activities and stored materials. Because the messages are stored on the employers' hardware, the potential review and disclosure of such messages raises a number of privacy issues. While the legislation may differ among the states, federal laws generally indicate that monitoring of business communications systems may be accomplished if necessary for the continuing operations of the business, and if the employees and other exposed parties are made aware of the extent of monitoring.

Federal wiretapping laws afford many employees protection from having their email and voice mail monitored. Specifically, Title III of the Omnibus Crime Control and Safe Streets Act of 1968[6] [6] (also known as the federal wiretapping statute) and the Electronic Communications Privacy Act of 1986,[7] (ECPA) outlaw the interception, use, or disclosure of protected wire, oral, and electronic communications [7].

There are, however, a number of important exceptions to these acts, which are relevant to many kinds of employers. For example, if an employer has a system that can be accessed by a wide range of users, such as a bulletin board, employer review of communications associated with the bulletin board would not violate the ECPA. Likewise, if an employer intercepts communications using a telephone extension and there is a legitimate business purpose connected to it, the employer's actions would be legal. Thus, if an employer has reasonable suspicions about an employee releasing trade secrets to a competitor, an

THE POLICY SHOULD STIPULATE HOW, WHEN, AND BY WHOM THE POLICY IS REVIEWED, AS WELL AS HOW END USERS CAN MAKE REVISION SUGGESTIONS.

[6] Codified as amended Title 42 U.S.C.A. 3768 et seq.
[7] Title 18 U.S.C.A. 2510 et seq.

employer could monitor the employee's calls on a particular phone extension.

The ECPA also prohibits the unauthorized entry into stored wire and electronic communications. Currently, the law provides an exception to those who provide the service. Another exception, historically pertaining to telephone companies, allows them to intercept phone communications for reasonable business purposes. A business that supplies email or internal voice communications capabilities to its employees is in fact a "provider of wire or electronic communication service," as detailed in the statute. As such employers may be able to access email or voice communications in order to protect their property [7].

Lastly, the ECPA allows employers to intercept electronic communications if express or implied consent was given. The courts, however, have ruled that the consent must be clear, or if implied, must be more than mere knowledge of the employer's ability to monitor. This underscores the need to not only create an effective telecommunications policy, but to also insure that it is distributed and agreed to (by signature) by all employees. When monitoring systems that may affect external participants, such as customers or suppliers, those parties should be notified of any potential monitoring activity. This could be accomplished through the posting of a warning banner on email communications, or a recorded notice on voice systems.

The extent of actual monitoring can vary depending on the perceived need of the organization. It can range from unlimited monitoring, monitoring certain transactions, monitoring when impermissible activities are suspected, to no monitoring unless required by law. If criminal activity is suspected, legal counsel should be sought.

Virus protection. With the ever-growing threat to information systems and telecommunications links by malicious software programs (viruses), organizations should pay close attention to the need for protection from viruses. A requirement that all electronic files and messages received through the telecommunications system undergo virus scanning should be outlined as a prerequisite for permitted storage on company systems. If Internet access or some other download format is permitted, then the organization should invest in quality software to protect the system.

Physical security. Informally known as "lock and key" security, physical security extends to the degree by which organizations allow communications and information systems equipment to leave the presumed security of the organizational grounds. If businesses allow this equipment to be checked out by employees, then the policy should stipulate fundamental security concerns to prevent theft, damage, or loss.

Encryption. If the organization uses encryption mechanisms or allows employees to use them, how the encryption keys are maintained is vital to proper management of otherwise inaccessible materials. If employees are allowed to encrypt their own files, for privacy or other reasons, the company has the right to insist that the decryption tools are maintained in a secured business location, in case they are needed to monitor suspected unauthorized or criminal use.

Violations of policy. This section specifically addresses how behavior deviating from established policy is to be reported and admonished. Employees failing to follow these guidelines should be subject to a range of punishments, from administrative reprimand to criminal prosecution. The means used to evaluate suspected violations of policy are also clearly defined, to promote a fair and impartial investigation.

Procedures for reporting violations. Many system abuses are discovered by accident, and many others by internal systems controls; far fewer are discovered by independent, purposeful detection activities initiated by the organization [11]. To support employee reporting of system abuse, clear procedures should be detailed for reporting violations of policy.

Penalties for violations. The penalties for confirmed violations are usually related to the dollar value of assets to be protected, as well as the level of violation performed [11]. Penalties for violations can range from an oral warning to written warnings and, if necessary, termination of the employee. Since some violations might be criminal in nature, employees could be prosecuted by local, state or federal authorities. Employers should be cautioned not to make unverifiable statements about suspected employees, since such assertions could be the basis of a suit for defamation by the employee.

Policy review and modification. A policy is only good if it is timely. Unless this policy, like any organizational policy, is reviewed periodically and updated to reflect changes in technology and the business, it will quickly become obsolete. This segment of the policy should stipulate how, when, and by whom the policy is reviewed, as well as how end users can make revision suggestions.

Limitations of liability. The final segment of a telecommunications policy should be a section detailing legal limitations for liability and general disclaimers for misuse of corporate assets. This seeks to provide some degree of indemnification for the unauthorized acts of employees or outsiders who have misused the company's assets. Specifically, the statements should warn employees that the company will not offer legal protection should they misuse the equipment, and that in fact, the company will deliberately seek to hold them liable for the consequences of such acts. Thus, if an employer is sued and found liable for the unauthorized and illegal actions of its employee, the employer will seek indemnification from the employee for damages the employer may have incurred.

Conclusion

Good telecommunications management strategy should include the establishment of corporate ethical norms for computer use, a maintenance of employee awareness and training, the enforcement of computer crime laws, and the control of physical access [3]. Policies specifying conditions for proper use are called for as deterrents from violations of computer abuse, and system misuse [11]. **C**

References

1. Aquino, J. Chevron's road to settlement. *The Recorder*, March 15, 1995.
2. Bergeron, F. and Bérubé, C. End users talk computer policy. *J. Systems Management 41*, 12 (Dec. 1990), 14–17.
3. BloomBecker, J.J. Short-circuiting computer crime. *Datamation 35*, 19 (Oct. 1989), 71–72.
4. Lindup, K.R. A new model for information security policies. *Computers and Security 14*, 8 (1995), 691–695.
5. Milberg, S.J., Burke, S.J., Smith, H.J. and Kallman, E.A. Values, personal information privacy concerns, and regulatory approaches. *Commun. ACM 38*, 12 (Dec. 1995), 65–74.
6. Scoma, L., Jr. Developing a healthy security posture. *J. Info. Syst. Manage. 3*, 1 (Winter 1986), 61–62.
7. Seifman, D.H. and Trepanier, C.W. Evolution of the paperless office: Legal issues arising out of technology in the workplace. *Employee Relations Law Journal 21*, 3 (Winter 1995/96), 5–36.
8. Smith, H.J., Milberg, S.J. and Burke, S.J. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Q. 20*, 2 (June 1996), 167–196.
9. Stone, E.F., Gardner, D.G., Gueutal, H.G., and McLure, S. A field experiment comparing information-privacy values, beliefs and attitudes across several types of organizations. *J. Applied Psychology 68*, 3 (Aug. 1983), 459–468.
10. Stonecipher, K. Establishing a comprehensive microcomputer administration policy. *J. Info. Syst. Manage. 3*, 1 (Winter 1986), 15–21.
11. Straub, D.M. and Nance, W.D. Discovering and disciplining computer abuse in organizations: A field study. *MIS Q. 13*, 1 (Mar. 1990), 45–60.
12. WarRoom Research, LLC. 1996 Information Systems Security Survey. WWW Document; www.infowar.com/sample/survey.html-ssi, 1996.

Michael E. Whitman (mwhitman@kennesaw.edu) is an associate professor in the Department of Computer Science and Information Systems at Kennesaw State University in Georgia.
Anthony M. Townsend (amt@udel.edu) is an assistant professor in the College of Business at the University of Delaware.
Robert J. Aalberts (aalberts@ccmail.nevada.edu) is an Ernst Lied Professor of Legal Studies in the College of Business at the University of Nevada, Las Vegas.