new york state society of
NYSSCPA
certified public accountants

Home of the Trusted Professional
3 park avenue, at 34th street, new york, ny 10016-5991
212.719.8300 • fax 212.719.3364
www.nysscpa.org

May 29, 2009

Ms. Nancy Cohen, Senior Technical Manager
AICPA
IT Section/CITP Credential
220 Leigh Farm Rd.
Durham, NC 27707

By e-mail: ncohen@aicpa.org

Re: Exposure Draft – Generally Accepted Privacy Principles

Dear Ms. Cohen:

The New York State Society of Certified Public Accountants, representing 30,000 CPAs in public practice, industry, government and education, submits the following comments to you regarding the above captioned exposure draft. The NYSSCPA thanks the AICPA for the opportunity to comment.

The NYSSCPA's Technology Assurance Committee deliberated the exposure draft and drafted the attached comments. If you would like additional discussion with us, please contact Bruce I. Sussman, Chair of the Technology Assurance Committee, at (973) 422-7151, or Ernest J. Markezin, NYSSCPA staff, at (212) 719-8303.

Sincerely,

Sharon Sabba Fierstein

Sharon Sabba Fierstein
President

Attachment

new york state society of
NYSSCPA
certified public accountants

Home of the Trusted Professional
3 park avenue, at 34th street, new york, ny 10016-5991
212.719.8300 • fax 212.719.3364
www.nysscpa.org

COMMENTS ON

EXPOSURE DRAFT – GENERALLY ACCEPTED PRIVACY PRINCIPLES

May 29, 2009

Principal Drafters

Yigal Rechtman
Bruce I. Sussman

NYSSCPA 2008–2009 Board of Directors

Sharon Sabba Fierstein, *President*
David J. Moynihan, *President-elect*
Richard E. Piluso, *Secretary/Treasurer*
Barbara S. Dwyer, *Vice President*
Joseph M. Falbo Jr., *Vice President*
Elliot L. Hendler, *Vice President*
Margaret A. Wood, *Vice President*
Louis Grumet, *ex officio*
Scott M. Adair
Edward L. Arcara
John Barone
Susan M. Barossi
S. David Belsky
Thomas Boyd
Anthony Cassella
Cynthia D. Finn
Robert L. Goecks
David R. Herman
Scott Hotalen
John B. Huttlinger, Jr.
Martha A. Jaeckle
Suzanne M. Jensen
Lauren L. Kincaid
Gail M. Kinsella
Nancy A. Kirby
J. Michael Kirkland
Kevin Leifer
Elliot A. Lesser
David A. Lifson
Anthony J. Maltese
Mark L. Meinberg
Avery E. Neumark
Robert A. Pryba, Jr.
Joel C. Quall
Ita M. Rahilly
Judith I. Seidman
Thomas M. VanHatten
Liren Wei
Charles J. Weintraub

NYSSCPA 2008–2009 Accounting & Auditing Oversight Committee

Mitchell J. Mertz, *Chair*
Michael J. Aroyo
Robert W. Berliner
Edward P. Ichart
Thomas O. Linder
Rita M. Piazza
William M. Stocker III
Bruce I. Sussman
Ira M. Talbi
George I. Victor
Robert N. Waxman

NYSSCPA 2008–2009 Technology Assurance Committee

Bruce I. Sussman, *Chair*
Harvey G. Beringer
Gary E. Carpenter
Matthew Clohessy
David O. Daniels
Adam Dunning
Matthew Giordano
Mudit Gupta
Patrick Helmes
Lucas Kowal
Joel Lanz
Richard Lanza
Yosef Levine
Jennifer A. Moore
Bruce H. Nearon
Yossef Newman
Joseph B. O'Donnell
Karina Pinch
Michael Pinch
Michael A. Pinna
Yigal Rechtman
Robyn Sachs
Walter Schmidt
Sheryl Skolnik
Inga Sokolova
Mark Springer
Irwin Winsten

NYSSCPA Staff

Ernest J. Markezin
William R. Lalli

New York State Society of Certified Public Accountants

Comments on Exposure Draft–Generally Accepted Privacy Principles

The New York State Society of Certified Public Accountants welcomes the opportunity to comment on the AICPA Exposure Draft – Generally Accepted Privacy Principles.

General Comments

1. The overall concept and establishment of principles and underlying criteria are timely and appropriate to this business environment. We believe that this document will assist U.S. managers, auditors, and stakeholders in enhancing business transparency, both domestically and internationally.
2. The standard is consistent with our interest as CPAs in upholding and protecting the public interest. The ED authors should evaluate the standard as a possible basis for litigation against CPAs and other constituents who may be placed under undue burden to demonstrate compliance with a standard, the reach of which is wider than currently prevailing practices. Accordingly, the authors should clarify whether or not these standards will be considered the minimum level of required practice for data and information privacy.
3. Alternatively, the authors should clarify the scope and basis of the proposed Generally Accepted Privacy Principles ("GAPP") in cases against business entities that are in litigation over data and information privacy. The intent of the ED authors should be made known if it is to provide the proposed GAPP as a basis akin to U.S. Generally Accepted Auditing Standards.
4. The reference to Trust Services is appropriate (see page 73). However, the sample report discusses only privacy issues. It does not expand upon the assurance provided by Trust Services. Clarification is needed on the scope of services under the proposed GAPP and its relationship to Trust Services.
5. The proposed standard should include reference to existing standards such as:
    a. Payment Cad Industry (PCI) - a mapping between PCI and the proposed GAPP would be helpful because we have observed much overlap between the two frameworks.
    b. *The Gramm-Leach-Bliley Financial Services Modernization Act*, which regulates aspects of the operation of financial institutions and is universally adopted and enforced by the U.S. Federal Trade Commission.
    c. The Canadian *Personal Information Protection and Electronic Documents Act*, which regulates data privacy.

The ED should reference these existing legal requirements and the authors should evaluate whether there are any inconsistencies between these oft-applied laws and the proposed GAPP.

Specific Comments

6. On page 1, GAPP is said to be "developed to help management create an effective privacy program." Accordingly, GAPP is intended for use by management. The ED should also reference the establishment of policies, procedures, monitoring and reporting activities directed to those charged with governance, typically a board of directors or trustees, or a committee of the board . Including those charged with governance in the ED will enable the appropriate response when handling issues of complaints and escalation of complaints.

7. Starting on page 4, under the caption, "What Is Privacy?" the ED defines privacy as "the rights and obligations… with respect to … **personal information.**" [emphasis added] The ED continues by distinguishing between "privacy" and "confidentiality."

   a. We believe that releasing this ED without reference to "business privacy," known in the ED as "confidentiality," would be a missed opportunity to maximize the effects of a newly established GAPP. On page 5, the discussion of "Privacy or Confidentiality" continues with "unlike personal information, rights of access to confidential information… [is] not clearly defined." We propose that an entity define its own confidential information with the bias that classifying all such information as "Private" is the appropriate approach to take under the proposed GAPP.

   b. Accordingly, using a risk-based approach would enable such entities with privacy related obligations to prioritize their approach based on their risk tolerance and regulatory or corporate governance requirements. Some entities (e. g., technology companies) might be rich with proprietary information that would be considered "confidential" but not elevated to the status of "private." We propose that the ED allow such entities to differentiate their approach versus mandating that all entities utilize a "one size fits all" approach, regardless of their risk profile. For example, technology and manufacturing companies operate with vastly different requirements for protecting trade secrets and intellectual capital.

8. On page 7, the second principle is defined as follows: "Notice. The entity provides notice about its privacy policies and procedures…" This is a circular definition. Instead, we propose the following change "Notice. The entity **effectively communicates** its privacy policies and procedures…."

9. On page 7, the eighth principle of Security refers to "unauthorized access (both physical and logical)." We believe that the word "logical" is too narrow.

We would like to make reference to a standard Information Technology distinction between General Controls and Application Controls. Both physical access and "logical access" (however defined) are subsets of General Controls as defined by the Committee of Sponsoring Organization (COSO) and by the AICPA in numerous publications. We propose that references to these concepts be made in the ED instead of to "physical and logical" access controls.

10. On page 10, the activity of "Sustaining/Managing" should make reference to risk-based approach that entities and individuals take in order to decide on the actions they wish to undertake as part of this activity. Further, there should be reference to any monitoring and reporting activities that is related to management and sustaining activities.

11. On page 10, the External privacy audit makes reference to "chartered accountants (CAs) and CPAs." We believe that–

    a. CPAs should be spelled out as "Certified Public Accountants," in the same style as "chartered accountants" is spelled out.

    b. Reference to CPAs should be first, being that the majority of the constituency in the United States carries the CPA designation and not the CA designation.

12. Generally, the criteria the ED enumerates is comprehensive and successfully establishes the requirements against which managers (and Boards, as per our comment in number 2) should measured. Our comments in this section of the ED are as follows:

    a. Reference 1.2.4 should include the effects of monitoring or feedback from reporting that should have an effect on the risk assessment process.

    b. Reference 3.2.1 should require consent only prior to use. The language of "or as soon as practical thereafter" should be deleted. This language could place managers and auditors in a position of having to establish reason for consent to be waived because obtaining it was not "practical." Instead, only prior consent should be allowed under the proposed GAPP.

    c. Reference 3.2.4 makes reference to "consent is obtained before information is transferred **to or from an individual's computer.**" [emphasis added] We believe that reference to an individual's computer is too restrictive. Instead, we propose that it be replaced with "to or from any device or asset under an individual's control."

    d. Reference 4.1.2 makes reference to "Type of Personal Information Collected." Based on our comments above, Personal information should also include the "confidential" information from entities, based on the entities' assessment and designation of information as being equivalent to "personal" information. This change should occur whenever the term "personal" appears throughout the ED.

e. Reference 4.2.2 states that "Methods of collecting personal information are reviewed by management, legal counsel or both …" We see a weakness in this language because managers, not legal counsel, have the ultimate responsibility for adhering to the proposed GAPP. Accordingly, we propose a change of language to "Methods of collecting personal information are reviewed by management, sometimes assisted by legal counsel…"

f. Reference 4.2.4 states that "Individuals are informed if the entity develops or acquires additional information about them for its use." We believe that this may be impractical for the entity that collects information due to the magnitude and complexity of data often collected. Accordingly, and in conjunction with our comment (b) above, there could create a vicious cycle whereby informing individuals about additional information collected would be impractical and create an excuse to avoid notifying individuals about aggregation of data collected by entities. If an entity is adhering with GAPP and shares information with another GAPP adhering entity, the notice to an individual from the two entities and consent by the individual should suffice.

g. Reference 8.2.2 makes use of "Logical Access Control." As per our comment in item number 5, above there should be reference to COSO's General controls which clearly define Access controls.

h. Reference 8.2.6 relates to "Personal Information on Portable Media;" we propose the language be expanded to include "or device."

i. Reference 8.2.7 relates to "Tests of effectiveness of key … safeguards." We propose that reference also be made to two attributes of these required tests:

    i. The results of the tests should be reported to the appropriate level of management and those charged with governance.

    ii. These tests should occur in conjunction and coordination with formal monitoring activities.

    iii. The term "penetration test" should be clearly defined.

j. Reference 9.2.1 states that "Personal information is accurate and complete for the purpose for which it is to be used." We propose a reference here to the consent given by the individuals. This would be helpful because the consent of individuals will reflect an accurate and complete set of information.