BLUE RIBBON COMMISSION TO ESTABLISH A COMPREHENSIVE INTERNET POLICY

Meeting Summary from the August 23, 2000 Meeting

Commission Members Present:

- Sen. Carol Kontos, Chair
- Sen. Phil Harriman
- Linda Monica
- James Mays
- Marilyn Mavrinac for Sally Sutton
- Matthew Jancovik
- Michael Edgecomb
- Sam Levy
- Phillip Lindley
- Alan Brigham
- Dan Gwadosky
- Gary Nichols
- Dan Riley for Paul Russinoff

Commission Staff: Deborah Friedman, Darlene Shores Lynch

Re-convening of Commission and review of the Commission's charge: Senator Kontos welcomed the Commission members and thanked them for their willingness to continue to participate in this legislative study. Senator Kontos reviewed the charge of the Commission and pointed out that the issues the Commission did not work on during the last interim dealt mainly with on-line privacy and asked Commission members for additional issues to examine during this phase of the Commission's work. The following were additional suggested topics:

- Maine's "Right to Know" law vs. on-line privacy
- Digital divide and public access
- Municipalities' access to on-line technologies and funding for the Maine Governmental Information Network

Status of Commission recommendations: Commission staff reviewed the status of the recommendations the Commission made in its November 1999 report to the Legislature.

Uniform Electronic Transactions Act (UETA) - UETA was enacted as Maine law by PL 1999, c. 762, allowing electronic signatures relating to a transaction, and contracts formed electronically to have the same legal effect as their non-electronic counterparts, provided the parties have agreed to conduct the transaction electronically. The law applies to records and signatures relating to business, commercial and governmental transactions, except wills, codicils and testamentary trusts and records governed by the UCC other than consumer sales and leases. Staff noted that a separate law passed by the Legislature, PL 1999, c. 711, excludes certain real estate documents and powers of attorney from the operation of UETA. Staff also noted that recent passage of the Federal "E-sign" law may preempt parts of Maine's law. Staff provided Commission members with a copy of an article written by Professor Patricia Fry on the issue of UETA and its relationship to the new federal "E-sign" law.

Digital Signature Law - The Maine Digital Signature Law, which was enacted by PL 1999, c. 762, provides that a digital signature may, at the option of the parties, be accepted as a substitute for a manual signature. Once accepted, a digital signature has the same force and effect as a manual signature. Digital signatures used in a transaction with a
state agency must conform to rules adopted by the Secretary of State. The rulemaking process will begin soon and persons interested in participating or receiving notices should contact the Secretary of State's office.

**State acceptance of credit cards** - Maine law, 5 MRSA §1509-A, was amended during the last session of the Legislature to require state agencies to implement procedures for accepting payment of goods, services, fines and other fees by credit cards or other electronic means. Administrative fees involved in credit card transactions will be absorbed into agency budgets and no surcharges will be passed on to the consumer. In addition, the Bureau of Revenue Services and the Department of Professional and Financial Regulation are required to report back to the Business and Economic Development Committee and the Appropriations and Financial Affairs Committee by January 20, 2001 on the impact of the acceptance of payments by credit cards on each agency's budget.

**Maine Governmental Information Network (MGIN)** - The Maine Governmental Information Network Board (Public Law 1999, chapter 428) was created to enhance electronic data exchange among state and local governments and other providers of governmental services. The board oversees the computer network that connects individual municipal governments and other governmental service providers. The Office of the Secretary of State provides administrative support to the board and is responsible for all regular operations of the board. Chapter 428 also created the Maine Governmental Information Network Fund to carry out the purposes of the law. However, very limited funding of $1,000 for the biennium was allocated to the Fund. The Governor submitted a proposal in the FY 2000 Supplemental budget to fund the information network, but the funding was not approved. The Maine Governmental Information Network Board will be meeting to determine what proposal they will recommend to the Governor to submit in the next budget. The Commission members agreed to wait and see what recommendations the Board proposes before making any final recommendations concerning the MGIN. Commission members requested that a representative from the Maine Municipal Association and several representatives from municipalities appear before the Commission to discuss the issues surrounding electronic data exchange in municipalities.

**Updates on Agency actions**: The Commission heard from the State Treasurer's Office, the Department of Economic and Community Development and InforME concerning actions that these agencies have taken to enhance e-government since the Commission last met.

- **State Treasurer's Office** - Dale McCormick, the State Treasurer, updated the Commission on the state acceptance of credit cards and electronic payments. The Treasurer's office has done the following:
  - It has negotiated a lower VISA/MASTERCARD merchant fee of 2.15% (replacing the former rate of 2.34%). The agency is also negotiating with AMERICAN EXPRESS to receive a similar rate.
  - It will pay the merchant fees for all state agencies for FY 2001 to allow agencies that do not currently accept credit cards and have not included the expense into their budgets, to accept credit cards for electronic payments.
  - It has arranged for next-day receipt of funds from credit card companies. In the past, it has taken two days to receive receipts of funds.
  - It is working with People's Heritage Bank to develop the Treasury Automated Management Information (TAMI) System to allow greater acceptance of electronic payments. TAMI is scheduled for statewide implementation July 1, 2001.

These standards apply to non-InforME use of credit cards, although InforME is hoping to be able to use these agreements to leverage the same agreements for use of credit cards through InforME.

**Department of Economic and Community Development (DECD)** - Alan Brigham, Director of Policy and Planning at DECD, discussed technology-related initiatives that were approved during the last legislative session. These include the Single Sales-Factor Apportionment of Corporate income, One Maine Business, the Attraction Marketing Program, the Applied Technology Development Center System, the Maine Micro-enterprise Initiative and the Regional Economic Development Assistance Fund.

Mr. Brigham also updated the Commission on the progress that DECD has made with the consolidation of its websites. The Legislature approved a new Information Technology Manager position for the department, which will be
InforME - Tamara Dukes, the General Manager of InforME, reviewed the initiatives that InforME has undertaken since the Commission last met. These initiatives include: InforMe maintaining the state of Maine website and providing a single portal for services offered by the State; increasing e-government services, such as vanity license plate checks, the purchase of hunting and fishing licenses on-line and allowing on-line cross checks of drivers licenses; and increasing the number of e-government and e-commerce services available to the public. InforME also offers web design and technical support services to state agencies. Future initiatives which InforME will be undertaking include: on-line access to corporate and UCC records; on-line professional license renewal; on-line payment of traffic violations; and on-line vehicle registration renewal pilot program. Ms. Dukes mentioned that National Information Consortium (NIC), the e-government company that manages InforME, is establishing a web privacy coalition to identify minimum standards for privacy and is developing an independent private seal and certification program for government Internet applications and portals.

Review of Federal and National Activity:

E-signature law - The Electronic Signatures in Global and National Commerce Act ("E-sign") law was enacted by Congress as PL 106-229 and is effective October 1, 2000. The new law is similar to Maine's new UETA law. The law applies to business, consumer and commercial transactions. Under the law, electronic records and signatures, and contracts formed electronically have the same legal effect as their non-electric counterparts. A state law may modify the electronic contracting provisions of the E-sign if the law is:

- adoption of UETA, as recommended and approved by NCCUSL;
- adoption of additional exceptions to UETA, provided they are not inconsistent with E-sign; or
- a law other than UETA that sets forth procedures or requirements for acceptance of electronic records or signatures, provided it is not inconsistent with E-sign, is technology-neutral, and if enacted after E-sign, makes specific reference to E-sign.

Commission members asked staff to look further into the issue of Maine's UETA law and how the "E-sign" law may impact it. In particular, they asked for additional information on whether the consumer notices provision is preempted by E-sign.

Internet Taxation - Federal law (PL 105-277) currently constrains states from imposing any new tax on Internet access services or any multiple or discriminatory tax on electronic commerce until October 21, 2001. A bill to extend the prohibitions for 5 years, until October 21, 2006 (H.R. 3709), has passed the U.S. House of Representatives, but has not yet passed the Senate.

Federal and State proposals regarding privacy - Staff reviewed the on-line privacy legislation currently pending in Congress. Staff will continue to track the progress of these bills to see if they will have any impact on the Commission's work. Staff also reviewed state legislation in the area of on-line privacy. Virginia has enacted a law requiring every public body that has an Internet website to develop a privacy policy and privacy statement by 12/1/2000. Commission members requested a copy of the Virginia law as well as other states' legislation.

Uniform Computer Information Transactions Act (UCITA) - UCITA is a proposed model law that was created and approved by the National Council of Commissioners on Uniform State Laws (NCCUSL) in December, 1999. UCITA establishes a new commercial law for creating, modifying, transferring or licensing computer information, including the purchase of computer software, games, on-line databases, multimedia products and the distribution of information on the Internet. Two states, Virginia and Maryland, have enacted UCITA. Virginia delayed implementation of the law until October 1, 2000 and has established a study commission to review UCITA's impact on Virginia's libraries, consumers and businesses. The Commission members agreed that they would like to receive additional information.
about UCITA and would like to discuss it further at a future meeting, although they may not be able to study it sufficiently to make a formal recommendation to support or oppose its adoption in Maine.

Future meetings: The Commission set the following additional meeting dates:
· Meeting #2: Friday, September 8, 2000 / 9:00 a.m. - 1:00 p.m., Room 126
· Meeting #3: Wednesday, September 27, 2000 / 9:00 a.m. - 1:00 p.m., Room to be determined (Rooms in the State House are not available for that date)
· Meeting #4: Friday, October 20, 2000 / 9:00 a.m. - 1:00 p.m., Room 126
· Meeting #5: Friday, November 17, 2000 / 9:00 a.m. - 1:00 p.m., Room 126
BLUE RIBBON COMMISSION TO ESTABLISH A
COMPREHENSIVE INTERNET POLICY

Meeting Summary from the September 27, 2000 Meeting

Commission Members Present:

Sen. Carol Kontos, Chair
Rep. Tom Davidson, Chair
Sam Levy
Phillip Lindley
Linda Monica
Gary Nichols
James Mays
Tony Perkins
Sally Sutton
Dan Gwadosky
Michael Edgecomb
Alan Brigham

Staff: Deborah Friedman; Darlene Shores Lynch
Office of Policy & Legal Analysis

Following a welcome and introductions, the Commission proceeded with its main agenda item for the day: discussion on privacy of information on the Internet.

Presentations on Internet Privacy:

Center for Democracy and Technology (CDT): Commission staff presented information from the Center for Democracy and Technology, a non-profit group whose interests include Internet privacy. Paula Bruening, staff counsel for CDT, was invited to speak to the Commission, but last-minute schedule conflicts prevented her from attending. From conversations with Ms. Bruening, and from the Center's Website, staff gleaned the following comments and recommendations for the Commission.

Concerns about privacy of personal information are not new to society - they exist in the off-line world as well as the on-line world. In 1977, a federal study group proposed principles of fair information practices, which are now widely accepted by public and private sectors as principles for managing information. The principles are as following:

· **Notice/Awareness:** Consumers should be given notice of an entity's information practices before any personal information is collected. Information might include identity of the collecting entity, the uses to which data will be put; steps taken to ensure confidentiality, integrity and quality of data;

· **Choice/Consent:** Choice means giving consumers options as to how any personal information from them may be used; this often takes the form of an opt-out system (where information may be used unless the consumer explicitly opts out; or an opt-in, where information is not used unless the consumer consents);

· **Access/Participation:** This refers to an individual's ability to access data about himself and to contest the data's accuracy and completeness.

· **Integrity/Security:** Data must be accurate and secure. Data collectors can ensure accuracy such methods as using only reliable sources, verifying with consumers and destroying untimely data. Security involves managerial and technical protections against loss, unauthorized access, destruction, use or disclosure of information.
· **Enforcement/Redress:** It is generally agreed that enforcement is needed to ensure effective protections provided by the core principles. Enforcement may take the form of industry self-regulation, the creation of private right of action for persons harmed by violations; and government enforcement by means of civil or criminal penalties.

Ms. Bruening's recommendations to the commission are to focus on developing privacy policies for government websites and on offering consumer assistance. Although CDT doesn't discourage states from experimenting with laws to protect privacy, states must realize that the laws will have limited effect because of jurisdictional problems and the probability that federal legislation will preempt state efforts.

**Chris Caine, VP for Governmental Programs at the IBM Corporation** gave an overview of the future of the Internet, which has seen an exponential increase in use. The Internet of the future will be more mobile and more pervasive, entering every aspect of our lives. These trends will increase demands to respect privacy. Good business practices will incorporate respect for customers' privacy preferences. Those businesses that do not take into account those preferences will not succeed. Privacy protection involves action by data custodians (businesses, government and non-profits) as well as by the consumer, who must make his or her preferences known.

Mr. Caine reviewed the results of an IBM-Multinational consumer privacy survey, indicating that consumers are ambivalent about collection of data about themselves - they like the benefits of personalized marketing, but fear the loss of control over personal information. A survey of websites shows that most commercial websites have posted their privacy policies, while most governmental websites have not.

IBM has taken a leadership role in the area of privacy by doing the following:

- Deploying high-quality privacy standards;
- Advertising only on websites that offer privacy notices (as the 2nd largest advertiser after Microsoft, this can make a difference);
- Heading industry efforts such as Online Privacy Alliance and the Privacy Leadership Initiative;
- Helping develop privacy-enhancing technologies such as the Platform for Privacy Preferences (P3P); and
- Assisting business and government customers to establish privacy strategies and programs.

Industry can do better by:

- incorporating more fair information practices in their privacy notices;
- making privacy notices clear and conspicuous;
- increasing the adoption of online privacy seals, which provide 3rd-party monitoring and verification; and
- continuing to educate consumers and companies about privacy.

As for government, it too has a role, as follows:

- Lead by example: adopt leading-edge fair information practices;
- Consider e-government implications;
- Crack down on identity theft and fraud;
- Balancing citizens' privacy rights with government access to information;
- Support research and technology related to privacy;
- maintain a dialogue with industry;
- educate citizens;
- complete federal action to address medical and financial privacy; and
- ensure that any laws enacted are carefully targeted, dynamic (changing to meet changing technology) and incentivizing.
Mr. Caine's concluding thoughts are the following:

- Privacy is an issue relevant to both on-line and off-line information collection;
- A careful balance must be struck between market-based mechanisms, laws and technologies; and
- We're all in this together - we must all earn the public trust - business, government and non-profits.

**Kara LaPierre, NIC**, reviewed privacy policies relating to government websites. She said that, although the number of state government websites with privacy policies is relatively small, the number is increasing. Government websites differ from private sites in that the government is governed by Freedom of Information laws, and is not allowed to keep some information private. Also, to give personalized service to users, the government site must have certain personalized data. Government tradition is weak on opt-in/opt-out technology and on security. You can protect against people forming an entire profile of another person by always keeping certain data elements private.

**Discussion following the presentations focused on:**

- Looking at what other states are doing to create requirements for privacy policies.

  - The need for a consumer advocate within state government - to understand and advise on the management of government information and privacy. Some companies have a Chief Privacy Officer, whose role is to provide an overarching review and management of privacy. Sally Sutton suggested using the Public Advocate or the PUC as models; the CPO should be independent. The Bureau of Information Services within DAFS is undergoing a restructuring, and it is suggested that the Commission weigh in with Commissioner Waldron on the importance of privacy. Gary Nichols explained that some states have included privacy matters within there is office. Mary Cloutier, an audience members from BIS, explained that BIS does currently have statutory authority for confidentiality and does have a security officer.

  - Use of government information by law enforcement - there is concern that information collected for one purpose (e.g., through 911 for emergency location purposes) might be used for law enforcement purposes. Consumers may agree to use for 911 purposes, but not for others, such as law enforcement.

**Planning for Future Meetings:**

The next meeting is the previously scheduled meeting on October 20th. A make-up meeting for the cancelled September 8th meeting is scheduled for November 1st.

For the October 20th meeting, commission members asked to talk about the following matters:

- Definitions of "privacy", "confidentiality," and "security"

  - A review by the Maine State Bar Association on privacy/confidentiality and the Maine right-to know laws. Tony Perkins will talk with the MSBA and report back to the Commission

  - Advocate for use of fair information practices by state and local government and by anyone who wants to do business with them. Sally Sutton will work with staff on a statement, which will include Alan Brigham's suggestion that state sites not link to other sites unless those sites have appropriate privacy policies.

  - Information on Chief Privacy Officers/ consumer advocates - where might such a position be stationed (Public Advocate; BIS; independent?); what would such a position look like; how would it be funded? what other groups are looking at this

  - Setting up a forum to continue discussing these issues in the future: Sen. Kontos and Rep. Davidson will
come with a recommendation on what committee should deal with privacy issues in the future: a current standing committee? select committee? inter-committee group?

UCITA - members again expressed serious concerns about UCITA. The commission does not have time to fully explore and make a recommendation, but felt that they need to say something in case UCITA is proposed in the upcoming legislative session. A motion was made to recommend that, at a minimum, the Legislature not act on any such law in its upcoming session, but that further study was needed. The Commission asked for some general background on the issue before they take a formal vote, so that they can give the Legislature a better sense of why UCITA is so controversial. Tony Perkins volunteered to provide some background at the next meeting.

NEXT MEETING:

Friday, October 20th
9 am to 1 pm
Room 126, State House
BLUE RIBBON COMMISSION TO ESTABLISH A
COMPREHENSIVE INTERNET POLICY
October 20, 2000 Meeting Summary

Members Present: Senator Carol Kontos (co-chair); Sam Levy; Linda Lord for Gary Nichols; Phil Lindley; Jim Keenan for Tony Perkins; Jim Mays; Eric Bryant; Mike Edgecomb; Sally Sutton

I. Definition of Terms

Members reviewed a memo prepared by staff, setting forth typical definitions of the terms "privacy", "confidentiality" and "security." The purpose of reviewing definitions was to clarify the differences for purposes of Commission discussion. One member suggested a change to the definition for "privacy," to indicate that it is a right to conduct one's affairs without revealing information that the individual does not wish to be known by others, whether the revelation is compelled or not.

II. State Policy Regarding Privacy Policies and Use of Fair Information Practices

Commission members reviewed staff memos summarizing laws and proposals in other state that require state agencies and other public entities to post privacy policies on their Websites. The laws and proposals often prescribe the elements to be included in the policies, and may require a governmental entity to prepare a model policy for use by the agencies.

Members discussed how Maine might require posting of such policies on state Webpages. Sally Sutton suggested that the Commission recommend a law requiring state and local agencies, within an appropriate time frame, to post privacy policies complying with the fair information principles on their websites and that they link to private sites only if they include such policies. Sam Levy said he believed that the University is already taking steps to post such policies on its sites, but also expressed concern that such requirements not infringe on academic freedom. Other options to the limit on linkage were raised, such as including a warning and disclaimer stating that the links may not have the same privacy protections as the state sites, or providing a seal of approval for certain sites.

Eric Bryant pointed out the importance of educating citizens about the privacy policies, and about their threats to privacy. Commission members agreed that public education was an important element.

On the issue of Maine's confidentiality laws regarding information in any format, electronic or not, the Commission expressed an interest in having someone evaluate the laws to see whether they comply with the fair information principles that are being applied to information collected on the Internet. Possible reviewers include the University of Maine Law School and the Muskie Institute.

III. Structure for Ongoing Work on Privacy

Commission members had discussed at prior meetings the possibility of having a "chief privacy officer" or consumer advocate for privacy in state government. Staff reviewed information about other states and Canadian efforts to provide such a position. Several states have comprehensive privacy laws and designate an enforcing agency. On the federal level, the U.S. Department of Justice enforces the Federal Privacy Act, and Congress has a Privacy Council to advise them on privacy issues. Canada has a "privacy commissioner" whose role is to be an ombudsman for Canadians in their privacy concerns, to represent and advise the Parliament on those issues and to be the primary national resource for research, education and information on privacy.
Sally Sutton introduced a draft proposal providing a privacy advocate in Maine state government. The advocate would receive and investigate complaints about confidentiality of information and provide legal representation if necessary; make recommendations to policy-makers; assist public and private entities in the development of policies and procedures to protect confidentiality; conduct research; coordinate State treatment of personal data; and educate the public.

The draft was modeled after the Public Advocate's office and the long-term care ombudsman's office and the position is intended to be independent as possible. Eric Bryant raised the question of whether the advocate would have sufficient enforcement authority, and explained that more explicit language may be needed in the draft to authorize the advocate to sue to represent individual complainants. Ms. Sutton suggested that legal representation would not be a major role for the advocate, especially in the beginning. Most efforts in the beginning would go to developing policies and assisting state agencies.

Janet Waldron, Commissioner of Administrative and Financial Services, was asked for comment on the proposal. She noted that some aspects of the work of the proposed advocate might belong in different places. Consumer protection could be provided by the Attorney General's office. Policies regarding privacy and disclosure of information are already being addressed by the Information Services Policy Board (ISPB) within the Department of Administrative and Financial Services. Commissioner Waldron passed out copies of a draft policy that ISPB is working on. She also noted that there is a lot going on in state agencies right now regarding management of confidential information. For example, the Department of Labor has a federally-funded position to ensure confidentiality of unemployment compensation information. Many agencies have cross-agency confidentiality agreements. Perhaps state agencies need to do more to ensure the public that information is being protected.

Senator Kontos expressed concern that so many different entities seem to be involved in setting privacy policies, without coordination and without involvement of legislative policy-makers. She asked staff to develop a matrix showing the different entities. She asked for more information about ISPB and about the Chief Information Officer position within DAFS. Commissioner Waldron stated that the CIO position would be the link on legislative policy issues, but primarily mentioned technological matters such as setting statewide technology standards and reviewing state technology contracts.

IV. Security

Lynn Lyford from Electronic Data Systems Corporation (EDS) spoke to the Commission about security and cyber crime at the Federal level. Lynn informed the Commission about a recent White House conference on cyber crime and security and that the Clinton administration had filed legislation to fund cyber education and security. At the state level, the Attorney General of Texas has created an Internet Bureau to investigate cyber crime and security issues. The Bureau was created with an $800,000 grant from the Governor's office. In addition, Washington and Oregon have held cyber security summits. Lynn spoke to the Commission about the need for industry to cooperate and share information about cyber crime and security and she cited the following legal and structural barriers as to why parties are sometimes unwilling to share information with other parties: industry owns the information and is often unwilling to share with others, anti-trust initiatives and frivolous lawsuits.

Bill Hantjis, Director of Information Assurance Services at EDS, spoke to the Commission about the importance of cyber security. He stated that the Internet is vulnerable to attack and is used to host crime. In addition, the speed and "forced multiplier" effect of the online environment increases the concern about security. According to Mr. Hantjis, 75% of security breaches include theft of proprietary information, financial fraud, system penetration by outsiders, network sabotage and denial of service attacks.

Mr. Hantjis explained the information assurance process to the Commission He stated that security is not easy and requires on-going vigilance because of new technology. He also stated that a security system must be built from the foundation up and that the goal of a security system should be to provide trust because trust is the foundation of a secure environment. Bill explained the information assurance life cycle to the Commission. The steps in the life cycle are:
1. planning and assessment, including security planning and compliance, assessments and availability
2. protection for the security system, including design implementation
3. validation that the system works
4. training others on how to use the system
5. monitoring and management of the system

Dick Hinkley, Director of BIS and Ellen Lee, Network Services Manager for BIS, spoke to the Commission about Internet security in Maine state government.

Information Services Policy Board (ISPB) sets policies and the information systems office implements the policies. In addition, there is an Information Systems Managers Group, which consists of all IT managers within state government, which provides research, development and technical advice to the ISPB board. BIS also has information security analyst to assess and monitor security in the network. Existing security protections include: firewall, authentication, virus scanning and disaster recovery. Maine already has a lot of processes in place to protect information. Ellen gave a few examples in state government: the Department of Audit and the Department of Public Safety are both audited by federal agencies and therefore are required to have secure systems.

Dick Hinkley suggested that greater coordination and training between agencies is one area where there is still opportunity for improvement. Improved training and coordination would help to ensure consistency between departments and across branches. Currently, there is no active oversight of departments’ security systems, except for audits. BIS is currently undergoing a federal audit of financial information and physical security. Mr. Hinkley pointed out that audits are still catching up.

Jim Mays asked whether the department had considered out-sourcing the auditing and monitoring function. Mr. Hinkley said that in the long-term that might be the way to go. Concern was expressed that information about any weaknesses in the state's security systems not be revealed to the public.

V. UCITA

Attorney Jim Keenan, sitting in for Tony Perkins, gave a brief summary of concerns with the Uniform Computer Information Technology Act (UCITA). UCITA establishes a new commercial law for creating, modifying, transferring or licensing computer information, including the purchase of computer software, computer data and databases, games, multimedia products and the distribution of information on the Internet. It was drafted by the National Conference of Commissioners on Uniform State Laws (NCCUSL), but unlike other drafting efforts the effort to draft this uniform law was sufficiently controversial that one of the major participants walked away from the effort. UCITA is very broad and can apply to anything digital, including music and imagery. Among the concerns about UCITA are concerns about how consumers can understand and negotiate the terms of the agreement with the software developer in a timely manner; concern about changing sales to licenses and the impact on copyright law; self-help remedies that allow a licensor to pull the plug whenever they think they have the right; and the default rules that favor large developers of software.

Virginia, which is one of only 2 states that have adopted the uniform law, is reviewing the law before it comes into effect. Mr. Keenan cautioned that the Maine Legislature should examine UCITA carefully before taking action on it, if such a proposal comes forth next session. Commission members expressed similar concerns and anticipate making a formal recommendation to that effect at their next meeting.