Joshua Jason Lazarus
ECPA
Discussion of Title II of the ECPA

Note: I apologize that my part of the executive summary is separated from the rest of the summary – due to mail server malfunctions; I was unable to email my portion of the summary to my group member.

Executive Summary for Title II:
Title II's contribution to the ECPA is what has caused many early computer users to become alarmed. Title I's redefinitions of communications to include computer communications may have been frustrating to some, but it is the outlining of computer-based criminal actions in Title II that has caused the greatest uproar. Once again, I have chosen to present this discussion of the ECPA as if it is current legislation; turning the clock back to 1986 to analyze the impact this piece of legislation would have had on computer users and lab managers during the late 80's. Later or current legislation which nullifies or modifies the ECPA is not considered. Title II outlines the legal proceedings relating to data requests, unauthorized access and its penalties, civil actions due to violations of these regulations, and various other regulations that form a good outline of duties and rights of system administrators. Overall, information that is given here should only provide an informational base for what lab managers should be looking out for. To provide adequate protection not only for themselves but also their customers, lab managers should seek the services of a law professional. This will insure that the system administrator knows their rights and their duties pertaining to criminal investigations and data requests.

Main Report of Title II:

Title II adds a large amount of information to Title 18 of the United States Code, in the attempt to add computer-related criminal matters into U.S. legislation. The ECPA breaks down the discussion of these criminal matters into the following sections, of which each will be explained in greater detail:

Sec. 2701 – Unlawful access to stored communications
Sec. 2702 - Disclosure of contents
Sec. 2703 - Requirements for governmental access.
Sec. 2704 – Backup preservation
Sec. 2705 – Delayed notice
Sec. 2706 – Cost reimbursement
Sec. 2707 – Civil Action
Sec. 2708 – Exclusivity of remedies
Sec. 2709 – Counterintelligence access to telephone toll and transactional records

Section 2701. This section outlines that it is unlawful to gain access to unauthorized electronic services intentionally. Punishments are laid out in two different categories; commercial and personal. Those committing this crime for commercial gain can suffer

up to a 250,000 dollar fine and up to a year in jail with jail time increasing to 2 years for each time after the initial occurrence. Personal attacks are limited to a fine of five thousand dollars and no more than six months in jail.

Section 2702. This section outlines how companies that provide these services need to make sure that they do not openly divulge the contents that they are trying to hide. It also includes references to other sections of Title 18 that relate acceptable exceptions to keeping this information under "lock-and-key", which most likely include the sys admin and law enforcement agencies.

Section 2703. This provides access for law enforcement agencies to information less than 180 days old and also gives guidelines to retrive data even older than that. It also states that law enforcement does not have to ask permission of the user if a warrant is issued. If a subpoena or a court order is issued, prior notice is required. This section also outlines the types of information that can and cannot be released to other people other than law enforcement. It also outlines that law enforcement can ask for data if they have the permission of the user along with the other various methods that they have to sequester the data. Overall, it reminds the provider that law enforcement agencies do not have to have the permission of the user for most data retrieval. This section also protects those that provide these services from being part of an investigation of their own habits, which concerns me deeply.

Section 2704 – This section outlines how a governmental agency would go about asking for backup information from a provider. It states that the agency can ask for the backup, which will be made within 2 days of when the agency asks for it. Furthermore, the user doesn't have to be asked for permission immediately. After 2 weeks the provider can release the information to the agency if they haven't received notice of a challenge from the user. This section outlines a challenge and also states that notification of the user may not be required if the agency believes that it will cause damage to the backup or other parts of the investigation.

Section 2705 – This outlines the agency's ability to delay notification to the user to up to ninety days (or more if the court orders it) for a variety of reasons.

Section 2706 – This simply outlines that either by court order or by an agreement between the governmental agency and the provider a cost reimbursement can be provided for services rendered and time wasted.

Section 2707 – Rather briefly, this section describes how to deal with civil action against violators of these regulations. This basically gives admins a way to file a civil action if they themselves have been treated unfairly by these processes.

Section 2708 – Rather than paraphrasing, it's probably best to simply include this whole section: "The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for non-constitutional violations of this chapter."

Section 2709 – Due to possible "clandestine intelligence activities" by agents of foreign powers, the FBI can order (the order coming from nobody lower than the Deputy Assistant Director) information on customers and their activities. There is the obvious need to prove that there is necessity for this, but this information does not have to be provided to the system administrator. Furthermore, any queries as such cannot be divulged to anyone but those parties involved (i.e. the system administrator and the investigators).

To explain in detail what this act expects out of providers requires through legal advice from a law professional. In short, it requires that these service providers not only know what is expected of them but also expects that they know their rights. Title II sets up the "rules of engagement" between investigators and system administrators by outlining how data retrieval legally works, how much information should be logged along with other pertinent rules outlining interactions between these two groups of individuals. Title II expects that system administrators keep detailed (if not overly detailed) records of transactions, online behavior, names, addresses, along with any other pertinent information dealing with their customers. When considering setting up a computer lab, one must seek legal advice on matters such as the ECPA along with other pertinent technology-minded regulations. This insures that when sys-admins are asked to provide information in a manner unlike the ones explained above, they know that their rights have been breached. Seeking this legal advice and keeping it handy in the event of the possible subpoena or warrant is useful in insuring that the right methods are applied, and if they aren't, that the correct civil action against such violations is sought. Many have disputed that this act gives too much power to those governmental agencies mentioned involved. The true power of this act isn't in the wording; it is in the misinterpretations that can result from a layman's interpretation of the wording.
Consider the following: a FBI agent asks for data pertaining to a investigation. Without knowing your legal duties and rights, one might assume that any FBI agent can ask for information without your permission. This is where the misinterpretations of this act comes into play. Being an informed sys-admin is the key in understanding this act and it's rights and implied duties. You have the ability to seek civil action in those cases where violations have occurred.
As a side note, sys-admins seem to be overly protected, but I'm sure that it won't be long (in the context of 1986) until legitimate concerns will force lawmakers to reconsider the partial immunity this act has given to sys-admins that may be committing crimes themselves.

Overall, this brief description is exactly that – a description of what this act puts into law. It does not serve as a reference for lab managers; when confronted with such investigations, managers should have already contacted a law professional that can inform them of their rights and duties.