

## **KEY FEATURES OF THE MODEL COMMUNICATIONS SECURITY LEGISLATION**

In promoting the successful passage of model communications security legislation in Pennsylvania, Maryland, Delaware, Virginia, Illinois and Michigan, a broad-based coalition of communication service providers as well as content owners that use those services have stressed the value of the legislation as protecting e-commerce for the benefit of consumers, businesses and state and local governments. In addition to cable operators, that coalition includes local and long distance telephone carriers, the motion picture industry, cable programmers, satellite television providers, local governments and state and local law enforcement agencies.

**The model communications security legislation updates state telecommunications and cable security laws to accomplish the following objectives:**

- Provide comprehensive legal protection for all broadband and Internet based communication services from unauthorized access, receipt, transmission, decryption and disruption, thereby addressing not only outright theft or unauthorized acquisition but intentional disruption or sabotage of communication services and networks;
- Protect e-commerce networks, Internet based and other network transactions against intentional disruption or unauthorized access, thereby making them more legally secure for businesses and consumers; and
- Prohibit "unlawful access devices" so that the legislation better protects lawful consumer interface devices such as "smart cards" and security modules from circumvention by pirate technologies.
- Define "unlawful access devices" so that technological protection measures used to protect programming content are legally protected from circumvention.

**The model legislation achieves those objectives by:**

- Expanding the scope of the state laws to include legal protection for all the new broadband and Internet based services offered by all communication service providers regardless of the type of network facilities or technologies used to distribute those services;
- Broadening the types of illegal devices to include any hardware or software, or any components, primarily designed or used for unauthorized receipt, disruption, transmission, decryption or acquisition of any communication service without the express consent or express authorization of the communication service provider;
- Adding a second category of prohibited devices called a "unlawful access device" which is defined as any type of equipment, technology or software primarily designed, assembled, manufactured, sold, possessed or used for the purpose of defeating or circumventing any technological protection measures used by communication service providers and

programmers to protect data, audio or video programs or transmissions from unauthorized receipt, acquisition, access, decryption, disclosure, communication, transmission or re-transmission;

- Adding definitions of other key terms such as "communication device", "communication service", "communication service provider" so that they include broadband and Internet based or communication services offered over all types of technology platforms;
- Tiering of the criminal penalties by the number of unlawful devices involved in the violation so that manufacturers and distributors are targeted by the legislation. The model legislation is not intended to change the penalties for actual theft of service by individual end-users;
- Adding forfeiture, restitution and venue provisions to the criminal penalty section of the state laws; and
- Adding a civil action provision providing effective remedies, including the recovery of statutory damages and/or the defendant's profits by any aggrieved parties, including communication service providers and programmers.