

Several states are currently considering bills that purport to update existing laws against theft of cable and telephone service. In fact, several of these bills go far beyond that modest and uncontroversial goal. As written, these bills would apparently ban legitimate computer security measures that are used routinely by enterprises large and small.

For example, the bills would flatly ban concealing from a service provider the place of origin or destination of a communication. The language of the Colorado bill (HB 03-1303) is typical:

A person commits a violation ... if he or she possesses, uses, manufactures, develops, assembles, distributes, transfers, imports into this state, licenses, leases, sells, offers to sell, promotes or advertises for sale, use or distribution any communication device ... to conceal or to assist another to conceal from any communication service provider ... the existence or place of origin or destination of any communication that utilizes a communication device

Supporters of the bills may not realize that concealment of the origin or destination of messages is a legitimate security measure that is commonly adopted by corporations and individual users alike, so that a blanket ban on such concealment may seriously impair computer security efforts.

For example, most companies (and an increasing number of homes) place a “firewall” device at the boundary between their internal computer network and the Internet. These firewalls are usually set up to use a technology called Network Address Translation (NAT), to hide the source addresses of outgoing network packets and the destination addresses of incoming network packets. This is done for security reasons, to prevent a network eavesdropper from learning the addresses of critical computers – it is difficult for the eavesdropper to break into a computer if he does not know its address. Ironically, the very method that companies use to protect themselves against such attacks – concealing the origin and destination of messages – would be banned by these bills. NAT technology is included in many popular products, including essentially all popular Internet firewalls and all recent versions of Microsoft Windows.

The ban on concealing origin or destination of communications would also apparently prevent many legitimate uses of encryption. For example, suppose an executive was waiting in an airport lounge, and she wanted to use the airport's wireless network to send a confidential email message to a client. To protect the message against the possibility of wireless eavesdropping, the executive's computer would establish an encrypted connection to her company's network. The email would travel through this encrypted "tunnel" back to the company network, and would then be forward on to its destination. This prudent use of encryption has the side effect of concealing the email message's destination from the provider of the airport's wireless communication service; so it would apparently run afoul of a ban on concealing message destinations.

Law-abiding citizens often find that their security or privacy depends on their ability to conceal their communications from network eavesdroppers, and law-abiding technology vendors built products to help them to do so. It is easy to see how measures that hide information from eavesdroppers can also have the effect of hiding the same information from a network service provider. This is no reason to prevent law-abiding citizens from using well-established, legitimate technologies to preserve their security and privacy.