Internet Service Provider Security & Accountability Act of 2004

This bill, known popularly as ISPSAA, places requirements on US consumer Internet Service Providers to promptly respond to and block reported attacks originating from their networks. The initiative will be designed and administered by a combined industry/government/independent-expert group called the ISP Security Consortium (ISPSC).

A wide variety of Internet attacks are the cause of easily hundreds of millions, if not billions of dollars worth of damages yearly in the US alone. This is due to theft of intellectual property, lost business and productivity for network outages and emergency response & clean-up costs. These attacks may originate from lone hackers, clusters of computers launching a distributed denial of service attacks, or the mass propagation of a worm or virus. However, in all cases, a strong majority of these attacks utilize compromised home and business computers as launching points. While those charged with protecting business and infrastructure assets will need to increase IT security spending to protect their resources, a parallel response to block attacks near their source is needed in order to curb the massive increase in Internet attack frequency and intensity.

The ISPSAA requires service providers to respond to "claims" of Internet attacks originating from within their networks. After being notified of a claim, it is the responsibility of the ISP to block the outgoing malicious traffic in an expedient manner and take adequate steps to prevent the same host from launching additional attacks. If a single customer is responsible for a consistent flow of outgoing attacks, the service provider must terminate their service. For the purpose of this bill, consumer ISPs are any organization that provides Internet access service directly to individual users. This may include traditional consumer ISPs in addition to university and business networks.

This act places a responsibility of action on ISPs while shielding them from liability as long as they comply with the rules created by the ISPSC. In this way the act is similar to the Digital Millennium Copyright Act, which contains "notice and takedown" provisions requiring ISPs to first warn, and then block the Internet access of infringing customers. However, in the case of the ISPSAA service providers are not required to completely block a user's Internet access; rather they are only required to guarantee that the host is not registered as attacking another network within a specified timeframe. As required in the DMCA, ISPs must appoint a security "point of contact", who will handle security "claims" filed with the service provider. ISPs are also required to provide customer identifying information if the damages resulting from an attack are significant enough to warrant criminal or civil proceedings.

Failure to comply with these requirements means the ISP accepts liability for damages caused by attacks originating within their network. Compliance with the act exempts service providers from liability, both from the attack victim and from any customer whose traffic is blocked or denied.

The exact definition of an "attack" as well as the specific requirements for response time, "clean" time, and other details will be developed by the ISPSC. These guidelines will be continually reevaluated to maintain realistic requirements that provide tangible improvements for Internet security. The ISPSC will develop the requirements for submitting claims and also provide independent arbitrator to decide on disputed claims. This body is composed of a collection of Internet infrastructure and security stakeholders, including representatives from the following areas: ISP associations, major ISP companies, the Internet Engineering Task Force (IETF), consumer advocacy groups, and security/infrastructure related vendors (including Microsoft, Symantec, Cisco, Juniper and others. The ISPSC will be guided by the Dept. of Homeland Security's National Cybersecurity Division to assure that the steps taken by the group are appropriate for US national security needs. The make-up of this group is inline with the public-private partnership model presented in the National Strategy to Secure Cyberspace.

Only groups registered with the ISPSC are allowed to submit claims. Such groups may include service providers, corporations with large business networks, government/military agencies, managed security companies, and general Internet security advocacy groups (such as DShield, MyNetWatchman, etc). These groups must meet certain technical and good-standing requirements, as outlined by the ISPSC, to become registered. A pattern of spurious claims will be grounds for the revocation of a group's registration.

Note: This text is provided as is. Please do not contact the course staff with additional questions about the content of the legislation—any ambiguity is inherent to the bill and can be incorporated in your analysis.

For additional information, please refer to past class materials and the following links:

DMCA and ISP Liability:
http://www.nolo.com/lawcenter/ency/article.cfm/ObjectID/1902780E-68C9-436B-925AC37E42F4CD71/catID/1D5464D1-2A36-45C3-95897F115FEEB097

Internet Intrusions: Global Characteristics and Prevalence:
http://delivery.acm.org/10.1145/790000/781045/p138-yegneswaran.pdf?key1=781045&key2=0830555801&coll=portal&dl=ACM&CFID=20745542&CFTOKEN=19054426

Inferring Internet Denial-of-Service Activity:
http://www.caida.org/outreach/papers/2001/BackScatter/

MyNetWatchman:
http://www.mynetwatchman.com/