Michael Taylor
mbt@mit.edu

April 2, 2003

Honorable Members of the Massachusetts House of Representatives,

I would like to alert you to the grave consequences of passing House Bill No. 2743, entitled "An Act to Improve Broadband and Internet Security." An executive summary of the harmful effects follows:

1. This bill will render illegal telecommunications devices that many Massachusetts companies currently rely on for conducting business.

2. This bill will serve as the bedrock for enabling incumbent monopolies and oligopolies to tighten their grip on Internet, telephone, and cable services. This law directly enables monopolies to criminalize activities that they see as undesirable to their revenue streams. Additionally, it gives them the traction to enforce service contracts that will exploit their monopoly power and charge rates that are not proportional to the underlying cost of providing the services, but rather are proportional to the estimated wealth of the consumer.

3. The bill can be used to attack the democratic nature of the Internet and turn it into a closed system like existing telephone and cable services. The main reason for which the Internet has grown at the rate that it has is because it is not controlled by any small group of interests. Everybody is currently free to innovate and create devices and software that increase the usefulness of the Internet. This bill will enable telecommunications providers to control the usage and rate of progress of Internet devices and applications.

4. This bill will have a chilling effect on Massachusetts commercial and academic research. Researchers will have to worry whether they will be sued or censored for quote "creating plans for unlawful telecommunications devices" when conducting basic scientific research.

5. Similar versions of this bill are being actively lobbied right now to the states of Arkansas, Colorado, Florida, Texas, Georgia, South Carolina, and Tennessee. National and international corporations (many located in Hollywood, CA) have met with resistance at the federal level for passing this bill. They are trying to get in "through the back door" and get the legislation passed at the state level. It is probable that the principle beneficiaries of this bill do not live in the State of Massachusetts.

I will now talk about some of the details of this bill and show how they contribute to these harmful effects. First, let us examine the definitions of the bill:

A. Section 1, 35 defines a “telecommunications service” as “any service provided for a charge or compensation to facilitate the origination, transmission, emission or reception of .. data, video, audio or Internet access.”

B. Section 1, 78 states that a “Unlawful telecommunication device” is defined as “any telecommunication device which is capable of .. the disruption, acquisition, receipt, transmission, or decryption of a telecommunication service **without the express consent or express authorization of the telecommunications service provider**, including” .. “any device, technology, product, service or software…”.

Essentially, this bill’s definition of “telecommunication device” includes any program you might install on your computer that uses the Internet (“capable of receipt, transmission”), or any device that you might hook up to a cable or phone system. This includes existing devices like answering machines (“capable of transmission”, “receipt”), VCRs (“receipt”), TIVOs or PVRs (“receipt”), or devices that skip advertisements (“disruption”). This definition effectively gives the telecommunications service providers the ability to determine what devices and software are legal and illegal by not giving their quote “express consent.”

C. Section 1, 50 defines a “Telecommunication service provider” as someone who creates or transports any form of data. This means that this bill is giving many parties legal foothold to manipulate usage of these services.

Let us now examine in more depth some of the harmful effects that I have mentioned:

1. This bill will make illegal devices that many Massachusetts companies currently rely on for conducting business. Many Massachusetts companies now rely on telephone and Internet services to allow their employees to telecommute, i.e., to work remotely on their company’s corporate network while they are traveling or working at home.

A principle concern for these businesses is the threat that their communication will be intercepted by another party. This could include both corporate, as well as international, espionage. Vital to maintaining the security of their efforts is the use of VPN “virtual private network” software and devices, as well as tools like “SSH” and other encryption software that prevent third-parties from spying on traffic. Making devices like this illegal will prevent companies from telecommuting. The section of the bill that prevents the usage of these devices is Section 2, line 18:

“Whoever possesses, uses, manufactures, assembles, distributes….any unlawful telecommunication device to conceal .. the place of origin or the destination of any telecommunication shall be punished by a fine …”

These devices have the effect of concealing the destination of communications, and thus would be rendered illegal by this bill.

Ironically, this section of the bill is in direct contradiction of the bill's intended purpose: "to Improve Broadband and Internet Security." Additionally, this section allows service providers to prohibit Internet anonymity services. For instance, consider rape victims or people with diseases like AIDS who will be discouraged from consulting Internet reference sources because they are prohibited from quote "concealing the destination" of their telecommunication. In many ways, the Internet is a reference source, much like a library. This bill, if applied in analogy to the library, would prevent people from walking into the library and browsing a book without having their action recorded by the librarian. Another rather Orwellian ramification is that this bill requires that telecommunications companies be informed of the source and destination of every email that one sends. Why should they be entitled to this knowledge?

2 & 3: As previously stated, this bill effectively gives service providers the ability to determine what devices and software are legal and illegal by not giving their "express consent." Effectively, the legality of devices is not codified in the state law, but rather by the whims and desires of telecommunication service providers. This enables service providers to conduct surveys to determine the economic backgrounds of different usage patterns of the Internet. Because this bill enables companies to prohibit the use of encryption software, this means that, much like airlines, these companies can examine usage patterns (e.g., business travel or online purchases) and correlate them with the income level of the individual. Imagine service contracts that charge extra based on the number of dollar signs used in an email, or the dollar value of goods purchased online.

4. Section 2, line 34: "Whoever possesses, uses, manufactures, assembles, distributes .. any plans or instructions for making or assembling any unlawful telecommunication or access device .. to allow [these plans] to be used or employed…shall be punished…"

Since unlawful telecommunications devices are defined by the telecommunication service provider, this component means service providers can arbitrarily determine that legitimate academic or commercial research constitutes "plans for unlawful devices." Providers can use this to legally intimidate researchers who are working on legitimate research that may embarrass or threaten the commercial interests of the company. This strategy has already been employed by music companies (the RIAA) to intimidate researchers like Princeton Prof. Ed Felten to retract legitimate research from publication.

In conclusion, I have mentioned only a small portion of the inherent problems with this bill. If the honorable Members of the House of Representatives intend to pursue this bill, I recommend that they assemble a committee of non-partisan economic, consumer rights, and technological experts to examine its impact and limit the scope of the bill to address the real needs of the citizens of Massachusetts.

Michael Taylor
Doctoral Student
Electrical Engineering and Computer Science
Massachusetts Institute of Technology