

From: Cronin John
Posted At: Wednesday, April 21, 2004 4:19 PM
Posted To: spywareworkshop2004
Conversation: Spyware Workshop - Comment, P044509
Subject: Spyware Workshop - Comment, P044509

Regarding the subject of Spyware, please note:

It will probably prove to be very hard to develop a legally sound definition of spyware. This is a problem that can have many attributes. Some of the attributes exist for legitimate purposes.

It will probably prove to be more productive to quantify the undesired results of internet use. These uses would not be limited to website advertising or spyware. New regulations would be better served if they eliminate the PROCESS of undesired behavior.

The following addresses means to manage the majority of the problems...

In the course of using the internet, no website or other internet service should install unrequested software or change the configuration of the user's computer. The functionality of the user's computer should never be altered from use of the internet.

Any unrequested modification to a user's computer should be viewed as vandalism and carry comparable fines and penalties.

No internet service or website should store a users personal information in a form that can be accessed, read, and/or exploited by another service or website. If a service or website stores this information, it must be responsible for its security.

It is strongly recommended a common service be created to manage the personal information that could be needed by an internet service or website. This managed service could then be controlled by the user. Access to the information would be allowed only at the expressed permission of the user.

There is existing internet technology that will make the creation of a common service relatively easy. The regulations should empower an organization, perhaps NIST, to work with the IETF to create new internet standards for this common service. All internet software, services, and websites should be given 2 years time to support the new standard after it is published.

Currently when personal information is collected it is stored without the user's knowledge and can be accessed at anytime without the user knowing it. By setting up a means to manage the information and requiring the user be asked for permission everytime the data is accessed, most of the privacy abuses can be thwarted.

No internet service or website has the need to scan a users computer indiscriminately for files and data. Some files may be downloaded (cached) and reused to improve the operation of the service or website. All internet services and websites should limit their access to data on a users computer to only those files required to operate the service or website.

Any attempt to access data on a users computer not provided or managed by the internet service or website should be viewed as theft and carry comparable fines and penalties.

Manufacturers of software to access internet websites and services should be REQUIRED to improve their products to control and restrict access from the internet to the users computer files, data, and configurations.

It is not technically difficult to implement restricted access to a computers data. The manufacturers should be given no more than 1 years time to upgrade their products to comply with the new regulations.

If you implement these recommendations, you will circumvent the mechanisms used to collect personal information illegitimately. These recommendations, as worded, will apply to a variety of internet services. Services would include websites, email, chat, and other applications. ANY service can be exploited to access personal information and/or harm a user's computer. By defining the rules broadly, you can provide protection for many internet services.

John Cronin