**Analyzing leakage of personal information by malware**

From the information that I have gathered from this article, adware is an issue that negatively impacts the privacy of user’s on websites they search for online. Adware is defined as the advertising that we see on websites that collect our information without our approval and interfere with the user’s ability to read the website by moving them to other pages, as opposed to the advertisements that are legally made and prompted on a website on the side panels that have been bought by advertisers to promote their product, which can be closed. Another major issue regarding adware is the fact that many of them collect user’s behaviors online and could contain information such as their spending habits or political views, which is puts user’s at risk for having that sensitive information leaked. This leads to potentially unwanted programs (PUP’s) to be added to our devices that could be used to further monitor our information to keep promoting ads that suits to our interests. In summary, while extensions (programs we willingly allow on our devices to promote ads) and adware share similar properties, the execution of adware collects our data into private files which has a chance to leak that personal information to potential groups that could harm the livelihoods of many users.

**Marketing and Internet Professionals**

In modern day internet, the passive collection of our personal information is an ethically controversial topic in commerce technology. While there are many programs that have been designed as a means to only show you potential advertisements a user might be interested in, there is also the risk that the personal information that has been curated for that user could be leaked, such as sensitive account information. With the current changes in the cultural climate of society, many leaders in technology and commerce are trying to adapt to these arising issues by establishing a census related to setting regulations on what these companies can do with our information and how they are held accountable for it. Planning for the future, many of the current plans that are being implemented into the market have started to establish basic principles that all business’ in the Internet world have to abide by in order to remain within the guidelines of the established rules that will be developing in the near future.

**Regulating Spyware**

This is an excerpt from a paper on the general governance on the Internet, and how legislatures should proceed with making new laws and regulations involving Internet based activities. It is case study made in the Berkeley Law Journal on how the recent regulations involving adware and spyware has caused different implications that could impede many enterprises that plan to establish themselves with an Internet based platform as the popularity has been exponentially rising over the last decade. This entry highlights the advantages in establishing a more harmonized, commerce friendly environment for rising business’ as more platforms that could help the economy rise has always been looked upon favorably if they are established in an ethical manner. However, it also highlights the potential dangers for programs like adware that hinder a user’s private and financial information. It leads into the topic of how the government can experiment with new policies to adapt to the expansion of the Internet without hindering the livelihood of the nation. In short, the Internet has a generally favorable impression to the growth of nations in commerce, however consistent regulations need to be established at a similar rate to how much the Internet is changing alongside those policy’s.

Sources:

Urban, Tobias, et al. "Analyzing leakage of personal information by malware." Journal of Computer Security 27.4 (2019):459-481. <http://ucelinks.cdlib.org:8888/sfx_local?sid=CAPTURE:CAPTURE&month=07&atitle=Analyzing%20leakage%20of%20personal%20information%20by%20malware&issue=4&title=Journal%20of%20Computer%20Security&issn=0926%2D227X&genre=article&date=2019&day=18&volume=27&spage=459&epage=481&aulast=Urban&aufirst=Tobias&auinit=T>

Marshall, Kimball, and Nansi Swartwout. "Marketing and Internet Professionals." Journal of Internet commerce 5.3 (2006):109-126.

[http://ucelinks.cdlib.org:8888/sfx\_local?sid=CAPTURE:CAPTURE&date=2006&genre=article&issn=1533%2D2861&volume=5&day=18&title=Journal%20of%20Internet%20commerce&issue=3&atitle=Marketing%20and%20Internet%20Professionals%27%20Fiduciary%20Responsibility%3A%20A%20Perspective%20on%20Spyware&month=10&spage=109&epage=126&aulast=Marshall&aufirst=Kimball&auinit=K P](http://ucelinks.cdlib.org:8888/sfx_local?sid=CAPTURE:CAPTURE&date=2006&genre=article&issn=1533%2D2861&volume=5&day=18&title=Journal%20of%20Internet%20commerce&issue=3&atitle=Marketing%20and%20Internet%20Professionals%27%20Fiduciary%20Responsibility%3A%20A%20Perspective%20on%20Spyware&month=10&spage=109&epage=126&aulast=Marshall&aufirst=Kimball&auinit=K%20P)

Menell, Peter. "REGULATING "SPYWARE": THE LIMITATIONS OF STATE "LABORATORIES" AND THE CASE FOR FEDERAL PREEMPTION OF STATE UNFAIR COMPETITION LAWS." Berkeley Technology Law Journal 20.3 (2005):1363-1432.

[http://ucelinks.cdlib.org:8888/sfx\_local?sid=CAPTURE:CAPTURE&title=Berkeley%20Technology%20Law%20Journal&issn=1086%2D3818&date=2005&genre=article&day=1&volume=20&month=6&atitle=REGULATING%20%22SPYWARE%22%3A%20THE%20LIMITATIONS%20OF%20STATE%20%22LABORATORIES%22%20AND%20THE%20CASE%20FOR%20FEDERAL%20PREEMPTION%20OF%20STATE%20UNFAIR%20COMPETITION%20LAWS%2E&issue=3&spage=1363&epage=1432&aulast=Menell&aufirst=Peter&auinit=P S](http://ucelinks.cdlib.org:8888/sfx_local?sid=CAPTURE:CAPTURE&title=Berkeley%20Technology%20Law%20Journal&issn=1086%2D3818&date=2005&genre=article&day=1&volume=20&month=6&atitle=REGULATING%20%22SPYWARE%22%3A%20THE%20LIMITATIONS%20OF%20STATE%20%22LABORATORIES%22%20AND%20THE%20CASE%20FOR%20FEDERAL%20PREEMPTION%20OF%20STATE%20UNFAIR%20COMPETITION%20LAWS%2E&issue=3&spage=1363&epage=1432&aulast=Menell&aufirst=Peter&auinit=P%20S)