ITMG

by Student Name

Submission date: 24-Apr-2021 03:46AM (UTC-0700)
Submission ID: 1568470111
File name: ITMG.docx (29.86K)
Word count: 1320
Character count: 6674

The Internet Spyware Prevention Act

Student Name

Institution affiliation

The Internet Spyware Prevention Act

Introduction

Position: In support of I-Spy as a beneficial law that imposes restrictions on spyware creators.

Thesis Statement

> The creation of this law is beneficial toward the current and future security of the United States and its citizens, enforcing this law prohibits excessive information cataloging and manipulation, as well as preserve limitations against malicious foreign actors posing as citizens.

The digital age brought a new meaning of surveillance and observation, before the era, it meant having agents or private investigators hold a close observation of someone physically to observe their expenditure of time and money. However, this has changed over the year, now surveillance involves smart devices interconnected to form the internet. The kind of surveillance experienced in the new era of technology is a nuisance and causes a lot of privacy breaches. According to Lofgren (2007), 90 percent of computers that are used in the United States of America are infected with a form of spyware with malicious intent. With an approximate expenditure of $2.6 billion in trying to block the spyware. It was with this in mind that in 2007 the honorable Zoe Lofgren representative of California district 19, honorable Bob Goodlatte who was a lobbyist by then, and honorable Lamar Seeligson Smith who was a representative of Texas district 16 came up with the I-SPY act of 2007 as an amendment to Title 18 of the USA code. The intentions of the act were to safeguard the American People against internet spyware of all kinds and from spending so much money on trying to prevent the spyware from taking their information.

The act was intended to prevent malicious behavior of individuals and not the technology used in the process, however, the specific act had major loopholes. The act could be used by intelligence bodies such as the FBI and NSA to access personal data from the users without any repercussions as it would be deemed examining the conversations and online histories to determine the malicious actors. The process of doing these observations and examinations was called “backdoor” surveillance.

Another loophole will be to enable warrantless surveillance of users from other territories who are not in any relationship with the United States of America. It was to be implemented using information collected from huge telecom companies such as Google and Microsoft. Once the data is obtained, its use was not in any way specified in the act even if the intention of gathering such information were to get to determine malicious actors. A great danger lied in this provision.

According to Gross (2007), the major target of this law is the people behind the technology that steals information, in essence, there is no way the technology can steal the information without users. The people behind the spyware include the advertisement corporations in order to acquire information that is actionable in the market, they do so by obtaining usage patterns of device users, search history, purchase history, and among other things example of such corporation include Google Inc., Microsoft Inc., and others. The other class of people who the law targets are the malicious actors or as they are commonly known, the hackers. Hackers obtain information from protected computers with the intention of using it to arm the user financially or physically or in another form. They can use various methods to obtain data including spyware that can take screenshots of the opened screen or a small video of the activities of your screen while using it without the user consent or knowledge, as stated by Super Admin (2005). Their acts amount to a

violation of the law. The third group of people who will be affected by this law is the spy network, there exists a different law on spying but the kind of spying intended here is the spy through the internet. Most spies act in the interest of foreign countries and may steal important information to give it to their country or sell it on the black market. Definitely, they access this data from protected computers without permission.

The penalty for breaking the law is jail time and fines to corporations, individuals, or companies. The penalty is for anyone who gathers information illegally which is protected information. The protected information includes credit card numbers, addresses, bank data, and personal numbers, social security numbers, and other personal data such as passwords (Rouse, 2010). The maximum jail term for breaking the law is 10 years.

The constitutionality of intruding on the privacy of citizens by the government has been challenged in court by quoting the fourth amendment and how it is relevant to surveillance. Such cases include the case of *Olmstead v. the United States,* where the supreme court was supposed to determine the constitutionality of wiretapping, other cases include the case of *Keith v. the United States*. The court found that the fourth amendment did not cover protection from electronic surveillance. On the other hand, companies that rely on JavaScript to run their applications and websites have also challenged this law by arguing that they require cookies in order for JavaScript to run smoothly. Obtaining such cookies can amount to the breaking of the I-SPY act. The organizations and individuals opposing the act do so out of lack of the appropriate knowledge of spyware and how much they can impact their online usage, however, some do so because their business will run down.

Before the I-SPY act was a law, there were acts before it that had been brought to the senate with a similar agenda, such laws include the computer fraud and abuse act which was enacted in

the year 1986 as a modification of the already existed computer fraud law of 1984, which prohibited accessing of a computer without proper authorization. The act is similar to the I-SPY in that it was intended to curb the illegal access of user information but was different in that the 1986 act was to curb illegal access to unauthorized computers while the spyware firms might argue that they are not the ones accessing the computer but their software and that gave birth to the I-SPY to cover this weakness and loophole in the act.

The I-SPY act, however, has its own weaknesses too, it defines the access of unauthorized information and illegal use through mainly spyware terms. In 2005, Intermix Media Inc. was successfully sued for the use of spyware and settled with the New York Attorney General with a huge sum of money, but after that most companies have distanced themselves from calling their programs spyware. In 2003, PC Pitstop was sued by the Gator for defamation by referring to their programs like spyware. They settled outside court and PC Pitstop agreed to stop using the name spyware. This can present a challenge as technically, most spyware used today does not fit the description given by the act. They are, in fact, adware and the perpetrators do not acquire any information making it hard for this act to be used against them.

In the future, the act might need to be changed to cover most aspects of illegally accessing information either remotely or physically. Also, it should be improved to cover adware on programs, which do not take any information but uses what they gather to present relevant ads to users.

The I-SPY act serves to protect the citizens of the United States from manipulation, acquiring, or cataloging of information by organizations or individuals. The citizens might feel safer being online because of this law, in the case of *Robbins v. Lower Merion School District,* it was determined that the school used webcams to acquire very private photos of students, in the

future, because of this act, people might rest assured this won't repeat itself without interfering with their freedom as it does not fight the technology used but the people behind it.

ITMG

ORIGINALITY REPORT

2%	2%	0%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Rutgers University, New Brunswick Student Paper	2%
2	en.wikipedia.org Internet Source	1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		

ITMG

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6