Privacy versus security: personal data and internet use, is your privacy being er...

There are many Americans who are perplexed by the very topic of Internet Privacy as well as the security of their personal data. While the topics, privacy and security are clearly defined by Merriam-Webster's Dictionary as two different things, they possess the ability to work together while one does not encroach upon the other. While these are two different topics, there are some that make the mistake of using these terms interchangeably. There is a way to maintain not being observed while remaining secure.

Some fear that the mere use of the Internet is funneling their information to some huge database recording personal activity along with personal information. Others are conspiracy theorists as well and believe that internet use is coerced and a plan to track movement and habits. There are many 9/11 conspiracy theories including that the signals to the airplanes was hacked by the government so that the planes and their captains would be rendered helpless and not be able to avoid the eminent crashes. There are also those who view the need for privacy regarding personal data and security as able to coexist without cancelling each other out.

And on the other side of the coin, there are some (some technology professionals included) who feel that national security trumps the need and right of personal privacy when surfing the web. The nature of the privacy versus security issue is that many, even those in decision-making positions are not sure of the actual difference between security and privacy. Merriam-Webster's dictionary defines privacy as " the quality or state of being apart from company or observation: seclusion b: freedom from unauthorized intrusion privacy>, a place of seclusion, and also secrecy b: a private matter" (Merriam-Webster).

Merriam-Webster’s Dictionary also defines security as the following: “ 1 the quality or state of being secure: as a: freedom from danger: safety b: freedom from fear or anxiety” (Merriam-Webster). While there are many differing opinions on this topic, there is a growing contention of the belief that one does not have to be sacrificed for the other, that personal data and Internet privacy can be maintained while national security is kept secure. Many people do not wish to give up their privacy to ensure security and will fight for that very right.

President Thomas Jefferson is often quoted as saying “ Those who desire to give up freedom in order to gain security will not have, nor do they deserve, either one. ” (Jefferson). In that same vein, many technology professionals believe the same as there are those on the other side of the coin, believing that if you have nothing to hide there should not be a problem. This is a rather dangerous theory due to the fact that there can be various interpretations of “ what to hide”. If you are a terrorist certainly you don’t want to be tracked and want your privacy so that you can breach national security.

On the other side of the coin, what if you are simply researching information regarding terrorism for a research paper or it could be your job to research ways in which the terrorists are trying to stay ahead of the curve so as to remain undetected. Would this flag you unfairly and create a situation where your privacy has been breached when you had no malicious intent? Or would you simply be glad that the government was vigilant in pursuing security? There can be several different views on this topic.

The scenario above brings to mind an episode of the television program " Good Times" starring Esther Rolle among its many stars. The episode focuses on the fact that the youngest son (Michael) has been researching information for a comparative paper involving the differences between a democracy and that of a communist dictatorship. While doing his research he checked a book on Cuba and the application of its government. With the government investigating, his father lost his job and the family was being watched by the FBI.

Upon finding out that the interest in communism and Cuba was only a child's research for a school paper, the father got his job back, but the family could not shake the feeling that they were being watched un-necessarily. In the television episode, the government blatantly violated the privacy of the family in the effort to keep the country safe from " an unknown threat". Americans should not and do not have to give up privacy maintained in their usage of the Internet and/or personal data in order to maintain security from outside or domestic enemies.

Privacy, as a main focus is usually regarding protection from people who would do us harm (stealing our identities, theft, etc…), however there are also privacy issues that don't involve malicious intent. Privacy is also considered maintaining information that must be kept confidential from regular everyday law abiding citizens. This begs the question of which is more important, privacy or security.

There are many supporters and detractors for either privacy or security, however there can e a non-mutually exclusive existence of both and technology professionals are starting to make this a commonly known fact while attempting to implement policies based in the idea. The “ Shibboleth” project is making the application of the idea of implementing security while keeping your privacy possible. The basis of “ Shibboleth” is that web sites trust 3rd party sites to validate information without personally identifying an individual, therefore maintaining privacy (St. Sauver, 2008). An example of this would be a credit card holder accessing their credit card balance on a website.

The 3rd party company validates the user as either the cardholder or not without accessing any additional or identifying information. This type of process enforces security to the user while at the same time maintaining their privacy. As many stories fill the news of databases being compromised or government laptops being lost or stolen, the “ Shibboleth” project will win many supporters. However, even with privacy being protected and security being enforced, it is up to the consumer to be vigilant regarding their personal information in the same way.

Many internet users fill the web-sphere with personal information from Facebook to LinkedIn. These networks (professional and social) encourage users to divulge information about themselves that may end up being dangerous, especially for our youth. There have been stories of people killed or hurt because they posted a specific status on their Facebook page. This can be simply taken care of by using the tools already resident on the site (privacy tools). There are various ways in which personal data and Internet privacy can be maintained while keeping national security in top working order.

There are various sources that allowing this to be the case more than the theory on an individual user level, without packages such as the “ Shibboleth” software application. Utilizing the firewall in your Windows or Mac operating system is an excellent method of keeping out intruders. Also effective is utilizing different “ adware” or “ spyware” applications aid greatly in deterring infringement on your privacy while surfing the internet by keeping web sites from mining and inserting your information into a database. These applications prevent the website you may be visiting from either saving files to saving information from your computer.

When used in conjunction with an up to date anti-virus program, you are generally safe from being tracked by the internet. You may also encrypt your information when sending email that contains sensitive information, common in the finance industry. While speaking of email, one must also screen carefully what emails are opened and/or forwarded. The practice of not opening mail from an unknown source and using the blind copy feature when sending to a group of people will also lend protection to you as well as others.

When the “ I Love You” virus was unleashed, it was mainly perpetrated by forwarding and copying email addresses. There are also situations where, no matter how much security is in place, human error and manipulations may win. In the corporate world, this has been a long fought battle. Users want privacy at their workstations; however, they are required to abide by policies that are in place to protect the company (as well as them as users) from any outside threats. Policies are generally written and distributed but most often they are signed and put out of mind.

This happens in cases where passwords are given out, precautions such as locking one’s computer when away is not done, or something as simple as leaving confidential information out on a desk. Even though many people know what to do to keep their (as well as other’s) information safe, there are still ways that people at an individual level are allowing personal data to slip through the cracks as potential targets. There are companies that don’t require a password change at specific intervals. This is dangerous because there are password decryptors that can be run indefinitely or a file may be intercepted and passwords retrieved.

Online advertisers are also guilty parties of the invasion of your internet privacy. While many consumers know they should not divulge personal information on the internet, they do so at the offer of receiving mailing information and winning “ stuff” not realizing that their information is being sold to many vendors in the process. There is the coming of a “ Do Not Track” registry (similar to the “ Do Not Call” registry) is alarming many online advertisers. Many are saying that this will be the death knell of the adware tracking that goes on throughout many web sites.

There are also many companies that are taking large steps to protect your information online such as Verint Systems. Dan Bodner, Verint Systems president & CEO, says “ Organizations need to uphold the integrity of recorded interactions in context with security, privacy, and industry and legal regulations, including protecting customer data and information” (Bodner, 2010). Verint is providing security while maintaining privacy by adding an extra level of encryption for the data as well as options to not record some sensitive data.

For example, cardholder data may be encrypted because it contains sensitive information and sometimes capping the record at certain information. Three different network security analysts interviewed stated that they, along with others in the same industry believe that privacy need not be given up as a means of obtaining security. They believe that being vigilant with the tools on hand are actually the best methods of maintaining your privacy while boosting security on a corporate as well as a personal level.

This includes following your organizations rules to the letter regarding passwords strength, email security, and other measures. This also means on a personal level being smart about what you download and even which websites you visit. Gabriel Weimann states (in his book, “ Cyberterrorism: how Real is the Threat?), “ Even before 9/11, a number of exercises identified apparent vulnerabilities in the computer networks of the U. S. military and energy sectors” (Weiman, 2004). This is particularly interesting because in many people’s opinion, this could be the worst threat of all.

If a terrorist hits the energy grid, it would create power outages in the majority of the country or if the military network is compromised, there is no end to the damage that may be done (from tactical to weapons development). The Department of Homeland Security defines Cyber-Terrorism as “ the use of computing resources against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

These can be operations to disrupt, deny, corrupt, or destroy information resident in computers or available via computer networks”. The vulnerabilities, detailed in the publication cited above, include stoppage of cable, computer, satellite or telecommunications; monitoring of the aforementioned, changing or destroying programs, networks, databases, data; etc… However, it is definitely state as well (as is also pointed out earlier in this paper) that the main threat to security as well as privacy is an inside threat.

This may include angry or former employees, people not following security rules, incorrect data entry, and a host of other forms of either sabotage or just plainly not being vigilant enough. While I do see the government as able to protect our country from outside as well as domestic threats to our security, I am of the mind that there is room for maintaining privacy for our citizenry. If this is not maintained, then those that would attack us win whether they gain access or not.

To re-state my position, I will also re-state the quote by Thomas Jefferson, “ Those who desire to give up freedom in order to gain security will not have, nor do they deserve, either one” (Jefferson). We must remember those who fought and died as well as those who paved the way and created innovations in technology so that we may be provided security. We must value our privacy and fight to keep it.

Reference

http://www. quotationspage. com/quotes/Thomas_Jefferson