The Human Right to Privacy in a Virtual World
By: Tiffany Marie Halvorsen

September 17th, 1787, was the dawn of a new power among the nations of the world. The people of the United States of America were now free of a monarchy and subject only to their own Constitution. The United States Constitution was influenced greatly by the principle of the consent of the governed, in which the government's duty is to serve the sovereign people by protecting the three basic rights to which all citizens were granted: life, liberty and property.

Two hundred and twenty-seven years later, these rights have been complicated by the creation of a global community, commonly known as the Internet. The world today appears much smaller than it did to humans living in it centuries ago, due to the proliferation of online networks connecting humans across the earth, ultimately creating a database of human beings and their online actions through the World Wide Web. In this type of environment, one's property is more than a home that can be invaded or vehicle that may be hijacked; it is now words that can be clandestinely stolen, or personal information that can be unknowingly accessed. The Internet has provided thieves with a new source of information and wealth, and thus is responsible for undermining policy makers and stealing personal data from oblivious consumers.

Since the Constitution was written for a nation without online communities, and its Amendments were crafted for a physical world, the introduction of the Internet has challenged the right of privacy in the US. With the amount of internet-connected devices predicted to break fifteen billion by 2015, twice the population of humans on Earth, this virtual world is perhaps larger, in theory, than the physical world (Cisco 2011), and now is the time to question the ability of US policy to protect individual privacy in such a globally diverse, essentially virtual, community. However, personal privacy is only one side of the pyramid. Internet regulation may

play a role in protecting individual rights, but arguments against Internet censorship also present the issue of withholding valuable statistical information and breaking constitutional rights.

A major issue surrounding the idea of personal privacy and the Internet is whether one's personal information is even considered private once it has been uploaded to a host server. In some circumstances, this accessible information can prove invaluable. For instance, Facebook, a social hub and advertisement hotspot for anyone with an online connection, has provided lawyers with a plethora of evidence for defense in the courtroom (Semitsu 2011, Pannozzo 2012; Stanley 2010). For example, in 2009, Rodney Bradford was falsely arrested and accused of robbery. His defense lawyer used a Facebook status typed from his father's house at the time of the robbery as his alibi, and the district attorney agreed to drop the charges. Additionally, if citizens could enjoy complete personal freedom online, then so could the hackers, thieves, and corporate watchmen that now lurk around every corner in today's virtual world. However, Internet users argue that the use of online social media has questioned the limits of the Fourth Amendment—meant to serve as a safeguard against unwanted breaching of personal space or information—and the meaning of privacy. Facebook, the primary example, treats its users' posts as publicly shared information, stored on a third party database, and thus renders them viewable to questionable third parties that may use the information however they please (Bedi 2013). This is essentially the same as having your personal closet dissected by a third party, an example of what the Fourth Amendment is meant to protect against. To counter these opposing sides and multifaceted issues, new policies must be crafted to balance the criminals of this new world with the personal freedoms of innocent civilians.

There are also researchers trying to convince the public that accessing private information, in some circumstances, is highly beneficial to the majority. Aside from information

Internet users willingly offer to social networking sites, personal medical records stored on servers are used in medical record linkage studies, and thus present a positive use of private information obtained without consent. Linkage studies, which are responsible for most revolutionary medical advancements, enable medical researchers to utilize statutory collections of population health data obtained from medical institutions without individual consent for the benefit of the entire population (Stanley 2010). These studies may include knowledge of the upbringing of a medically ill child, or other environmental factors associated with a person of interest. Although this information may seem very private, obtaining written consent from all individuals in a population would present bias into any statistical study in which all persons unable to be located would contribute to significant error. So, should each person be victim to such a blind loss of privacy? Do the benefits of using said data for medical research outweigh the loss of privacy on an individual level?

Once again, there is another side to the story. New digital fingerprinting technologies developed by for-profit corporations are able to personally profile Internet users based on their browsing practices and sell that data to advertisers and marketers. One such technology is "Device ID" by BlueCava, an Internet marketing corporation. This software acts like a GPS tracker would, when secretly placed on one's personal vehicle, facilitate an accurate profile this person's every day travels (Sullivan 2012). The same idea applies to the controller of the Device ID. The CEO of BlueCava stated that Device ID has 99.7 percent accuracy at profiling personal devices (i.e., connecting an IP address to a user) and has thus far identified about 10 percent of the online devices in the world. This breach of personal privacy is one that clearly goes unnoticed and would thus seem to be unconstitutional. The issue here is how to regulate the unwanted use of personal online information that, to the consumer, seems unfair and

unnecessary, and yet still allow researchers to obtain the information they may need for linkage studies, which, in contrast, may seem completely beneficial.

Unfortunately, the fight over property rights on the Internet has already led to questionable data analysis practices by large corporations, perhaps an indication of what the future of the Internet may hold. Such practices are exemplified by the recent applications of "Big Data analysis" by Target, a technique involving the capture, storage, and analysis of huge amounts of consumer data collected by said fingerprinting technologies (Sullivan 2012). In 2010, companies spent $3.2 billion on Big Data collection, a number predicted to reach $16.9 billion in 2015. Target's use of consumer data, reported on in the New York Times Magazine, revealed how far the use of Big Data can go, and where it may be headed in the future (Sullivan 2012). Target developed a method for predicting the pregnancies of its female customers, perhaps even before the family received news of the pregnancy. This invasive use of personal information illustrates the improvement of corporate marketing capabilities. Machines loaded with terabytes of personal data on consumers can now be programmed to predict conclusions about individuals, aspects of human lives that should theoretically remain personal, such as impending pregnancy.

The Internet seems to be quickly turning into a battlefield between many components, some vying for money in the form of increasingly successful advertising and others for the unsurpassed usefulness of statistical information that may lead to remarkable medical advancements or proof of innocence in the court room. The Internet needs regulation in order for humans to maintain their basic rights. Amendments crafted for a world with extended property, online property, are the only solution.

Without a regulatory policy in place to protect against infringement of personal rights online, the Internet may never be a legally anonymous environment, but at what point is too

much surveillance breaking the promise of the 1st Amendment—freedom of speech and expression? The Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA), which sought to provide protection against piracy, led to activist uprisings criticizing the bills' potential to limit free speech and stifle innovation (Crisp 2013).

Is Internet censorship truly breaking any legality, though? There are many theories as to what facets of freedom the First Amendment may apply, some of which consider it valid only when one's speech involves betterment of democracy, and yet some distinguish between public speech—valuable to the greater majority—and private speech—used only for private gain and not for communal good (Johnson et al. 2009). Under these dispositions, Internet browsing and social networking may seem negligible and, thus, not private at all.

By some, the Internet is often regarded as a very democratic form of communication, allowing citizens the ability to use an avatar or online identity to actively participate in speechmaking and, more importantly, to be heard and to maintain their safety despite their opinions. Anonymity once provided a safeguard against privacy infringement while still allowing freedom of expression to take place, but technologies such as Device ID can now trespass even that protection, increasing the tension between freedom of expression and rights to privacy. Additionally, those with malicious purposes are also free to use anonymous identities online, increasing the chance of defamatory activity in the Internet. For example, the US Attorney General stated that "attacks on network frauds, software piracy, corporate espionage and trafficking in child pornography are just some of the crimes facilitated by the Internet [so] it is easy for a criminal to create a fictitious identity [and] this anonymity can significantly complicate an investigation" (Rowland 2003). In many court cases, though, a right to anonymity has been acknowledged, as it is the only reliable method for protection of privacy online. To

determine the role of anonymity in the human right of privacy as it is applied to the Internet, its impact on illicit and criminal activity against its ability to protect individual privacy must be carefully measured in such a way that the risks and benefits can be balanced. The Internet is no doubt a positive contributor to democracy, but without the proper regulation in place, it is a tool for criminality.

Thus, in conclusion, the new world community created by the introduction of networking to people across the earth has presented an opportunity to amend the Constitution to reflect the changes of basic human rights in this country. As more people "log on" with their Internet identities, there is an increasing amount of information available within this online community. Since corporations have learned how to exploit this information for profit, the issue is how to protect online identities against malicious hands, while maintaining the freedoms of speech and expression that are basic rights of the US citizen and allowing some information to be used statistically. The Constitutional Amendments must mediate a newfound balance between protecting the citizen online while still preserving the values America's forefathers built the United States upon: maintenance and protection of each person's life, liberty, and property.

Works Cited

Bedi, M. (2013). Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply. *Boston College Law Review*, *54*(1), 1-71.

Cisco (2011). Global Internet Traffic Projected to Quadruple by 2015. Cisco Visual Networking Index Projects Network. San Jose, CA.

Crisp, V. (2013). The piratical is political. *Soundings (13626620)*, (55), 71-80.

Johnson, B. H., & Youm, K. (2009). Commercial Speech and Free Expression: The United States and Europe Compared. *Journal Of International Entertainment & Media Law*, *2*(2), 159-198.

Pannozzo, A. L. (2012). Uploading Guilt: Adding a Virtual Records Exception To The Federal Rules of Evidence. *Connecticut Law Review*, *44*(5), 1693-1721.

Rowland, D. (2003). Privacy, freedom of expression and cyberSLAPPs: fostering anonymity on the internet?. *International Review Of Law, Computers & Technology*, *17*(3), 303-312.

Semitsu, J. P. (2011). From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance. *Pace Law Review*, *31*(1), 291-381.

Stanley, F. (2010). Privacy or public good? Why not obtaining consent may be best practice. *Significance*, *7*(2), 72-75.

Sullivan, M. (2012). Data Snatchers! *PC World, 30*(8), 77-85.