LAW, POLITICS, AND ONLINE SOCIAL NETWORKING

HONORS THESIS

Presented to the Honors Committee of

Texas State University-San Marcos

In Partial Fulfillment of

the Requirements

For Graduation in the University Honors Program

By

Alexander Ray Alfonso

San Marcos, Texas

January 2010

LAW, POLITICS, AND ONLINE SOCIAL NETWORKING

Approved:

_____
Dr. Heather C. Galloway
Director, University Honors Program

Approved:

_____
(Dr. Randall Osborne)
(Department of Psychology)
Supervising Professor

ABSTRACT

This paper focuses on legal and political aspects of online social networking which might contribute to negative societal affects. This paper seeks to answer the question, “Do online social networks contribute to illegal violations of the public’s privacy?” This study examines notions such as the permanent nature of internet content, the inverse relationship between online social networks and personal privacy, and the uncontrollable characteristics of user-generated content. The paper uses recent political debates to address prominent issues surrounding online social networks. An examination of politicians, partisan legislation, and political developments provides readers with an understanding of the political dynamics that govern legislation. Concepts, revelations, and findings derived from literary analysis are also used to conduct a real case study. By exploring two tort laws, this case study shows that online social networking can facilitate illegal invasions of privacy via the users and owners of online social networking websites.

ACKNOWLEDGEMENTS

This thesis would not have been possible without the time, encouragement, and patience of my supervisor Dr. Randall Osborne.

I would like to show my gratitude to Former Congressmen Fitzpatrick for his advice and enlightenment. Our discussions on the DOPA bill brought me to the realization that American law is inseparable from American politics.

I am grateful that Dr. Kens took the time to review my work; his insight was invaluable. I would also like to thank my mother for her continued support and intellectual encouragement. Her suggestion that I write about the internet sparked the initial interest of this thesis. Overall, I owe my deepest gratitude to the Texas State University Honors Department. I will always hold the honors classes that I took as the cornerstone of my education.

CONTENTS

INTRODUCTION

An online social network is an interactive computer service that allows its members to create, modify, and publish content about themselves and other people. Members of such websites are exponentially increasing. There are many online social networks available to the public such as Friendfinder.com and Linkedin.com, but the two most popular are Facebook.com and MySpace.com. This study intends to determine if and how online social networking can have negative effects on society.

When analyzing online social networking websites, the law can serve as a means of gauging their negative societal effects. This is because many democratic societies use the law as a means of condemning behavior and actions that are collectively considered inappropriate, inefficient, or dangerous. If something violates or contributes to illegal action, then it is likely that that action has some sort of negative effect. Therefore, if online social networking violates or contributes to violations of the law, then online social networking contributes to negative effects on society.

One of the main concepts that this paper attempts to establish is the inverted relationship between online social networks and the right of privacy. Because of this unique correlation between online social networks and public privacy, this paper will use privacy law to examine whether online social networks such as Facebook and MySpace contribute to negative effects on society. An examination of current tort law reveals that online social networks contribute to violations of prominent privacy laws such as the "Right of Publicity" (Winn & Wright, 2002, para. 1) and the “Public Disclosure of Private Facts." (Scott, 2006, para. 1)

It is often argued that the “relationship between politics and public law is a vexing one.” (Christodoulidis Tierney, p.1) The inextricable link between politics and public law makes it impossible to examine one without the other. Because politics can be enacted through law and the law is created through a system of politics, their independent examination does not provide adequate understanding. Therefore, this paper uses prominent political opinions, congressional voting data, and documented partisan voting patterns in an attempt to fully address the relationship between online social networks and the law. Examination of a political debate reveals that online social network legislation is a partisan battleground in which Republicans seek to restrict the use of online social networks and Democrats have sought to educate potential victims.

Online social networks tend to be altruistic, beneficial, and effective systems of communication. However, they can also contribute to negative societal affects. Even if a system is of massive benefit its potential risks and costs must not be ignored. Today alone, the online actions of every American will be documented and stored. Millions of children will submit personal information to online social networks, and thousands of adolescents will publicly post defamatory pictures that they cannot retrieve or delete. Although these facts are elaborately documented they often fail to permeate into the realm of common knowledge. It is a fore most goal to increase awareness by revealing such facts.

This body of work will establish four main concepts. It will show that private information cannot exist on the internet, the right to privacy and the expansion of online social networks are inversely related, online social network legislation is partisan and stagnant, and online social networks contribute to violations in privacy law.

ONLINE SOCIAL NETWORKS

What are Online Social Networks?

Online social networking is a virtual environment in which people from all over the world can interact and collaborate socially. There are several terms for online social networks such as social network sites, online networks, and social networking websites. In the most basic sense, an online social network is an online based service that facilitates some sort of interaction between its users. According to Danah Boyd and Nicole Ellison, online social networks provide "services that allow individuals to

(1) Construct a public or semi-public profile within a bounded system,

(2) Articulate a list of other users with whom they share a connection, and

(3) View and traverse their list of connections" (para. 4). Although the Boyd/Ellison definition of online social networks highlights some of their key characteristics, the comprehensive definition is somewhat restrictive. By defining an online social network as an online service that provides a medium through which users can interact and collaborate virtually, one can better analyze the full variety of current and future online social networks.

As their name might suggest, most online social networks revolve around interpersonal relationships. As Boyd and Ellison explain, "most sites support the maintenance of pre-existing social networks." However, many of the most popular online social networks have derived their success from connecting individuals to new social networks. It is important to realize that online social networks are intended to

appeal not only to the general public but to copious amounts of niche social segments. This is why there are currently hundreds of different online social networks. This is also why online social networks like Facebook and MySpace are constantly creating new applications and virtual activities.

Networks like Facebook and MySpace allow users to perform a plethora of virtual activities such as chatting, trading pictures, and playing collaborative games. It is likely that the success of an online social network is closely tied to its ability to provide a wide variety of unique applications.

The most successful networks tend to be those that allow their users to fully express themselves. Some online social networks have taken online communication from a means of transferring data into method of conveying contextually inclusive information. Online social networks provide such information by utilizing both subjective and objective forms communication. This is usually accomplished through various applications which operate within the online social network. For example, Facebook allows its members to express themselves subjectively through qualitative "update" statements and unique personal assessment quizzes such as "Which Candy Are You Like." Facebook also allows its users to express objective data by showing the quantity of friends each user has, the school the user went to, and the groups the user belongs to. One of the most popular applications on Facebook is one which allows users to create groups and causes. According to Boyd and Ellison, this enables a user “to articulate and make visible their social networks." (Boyd Ellison para. 6) Boyd, Ellison, and many others believe that association is a pivotal aspect of online social networking. A user’s

ability to easily express their associations is a key characteristic of many prominent online social networks.

Another unique attribute of popular online social networks is their use of profiles. Technically a profile is nothing more than a personalized website. In a way online social networks like Facebook and MySpace are HTML editors that make it easy for users to build personal websites about themselves. Ironically, many users don't even realize that they have their own website.

Most users think of profiles as a way of creating virtual representations of themselves. Profiles encourage members to publish large quantities of personal information online. Sundén put it perfectly when she stated that profiles "enable users to type one's self into being." (Sundén, 2003, p. 3) Through a profile, users can post pictures of their selves, post quotes, and create events. The profile is at the heart of most online social networks. The ability to express thought, feeling, and association is often considered to be a prerequisite for successful online social networks. Put simply, an online social network's success is directly related to expression.

History of Online Social Networks

The first prominent form of online communication was known as Internet Relay Chat or IRC. Internet Relay Chat "an online social channel" (Howard Rheingold p.14)" was invented in 1988 by Jarkko Oikarinen." (Howard Rheingold, p.14) IRC allowed individuals that were identified by an IP address to send text messages to other IP addresses. This early form of online communication had many limitations. For example, each user had to know the IP address of people they wanted to contact. In a way IRC was

like a pay phone. It allowed one to communicate but only to those whose number they knew. The restrictions of early online social networks like IRC created undefined networks. Unlike today's online social networks there were no established friends or social groups.

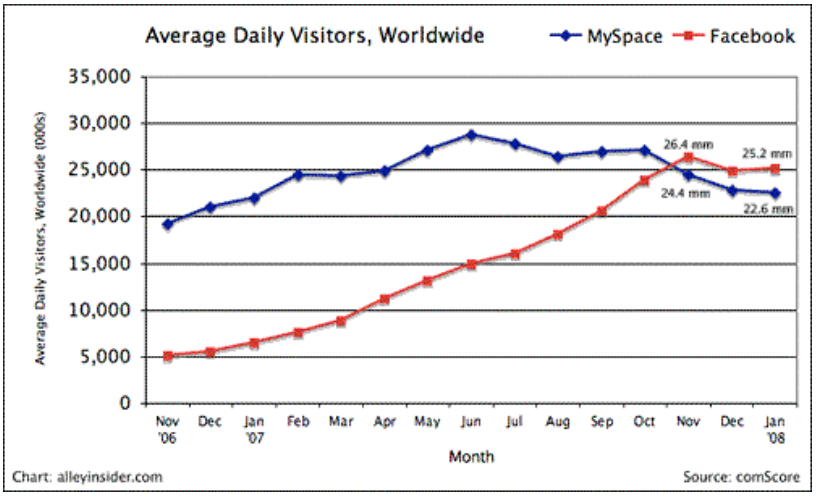
In the 90's chatting evolved when software developers created online chat rooms. The creation of chat rooms popularized the practice of chatting online. In 1996, online communication further exploded with the advent of Mirabilis' program ICQ. The program ICQ, which stood for I Seek You "can be considered the first modern, freely available instant messaging client for Microsoft-based workstations." (Paul L. Piccard, p.134) The program was revolutionary because it made it easy to find other users. ICQ also provided users with real time information about which uses were online. In 1997, ICQ would be purchased by America Online and developed into the modern concept of instant messaging.

Another popular trend that lead to modern mainstream online social networks was blogging. In Russell Kay's opinion, "The biggest impetus for social networking" ... "was the rapid growth of blogging." Like chatting, blogging serves as the basis for today's online social networks. A blog is essentially a website that allows users to post literary content. Blogs have been used as public journals and even personal marketing devices. Jorn Barger coined term "web blog" in 1997. The first "Website with blog-like characteristic was the National Center for Supercomputing Applications"(Meredith G. Farkas, p.14) which was created in 1993. In the early years, only people with the ability to program in HTML could create blogging websites. But as online social networks began adding blogging functions, the ability to blog was open to basically everyone.

According to Russell Kay, the first online social network was developed in 1995 under the name classmates.com. However, by following the Boyd/Ellison definition the first online social network, sixdegrees.com was created in 1997. By allowing "users to create profiles, list their friends and, beginning in 1998, surf the friends lists" (Boyd Ellison para. 10) SixDegrees provided the functionality of most modern online social networks. From 1997 to 2001 many dating websites such as AsianAvenue, BlackPlanet, and MiGente began modifying their services by adding social networking features. 2001 also saw an online launch of networks aimed at the business community. Systems such as Ryze, Tribe.net, LinkedIn, and Friendster linked users both "personally and professionally" (Boyd Ellison par. 18). Except for LinkedIn, most of these business social networks would become "one of the biggest disappointments in Internet history" (Chafkin, 2007, p.1) because of their failure to generate revenue.

The year 2003 saw the true rise of popular online social networks. This flux in popularity was closely tied to the rise of user generated content. Online Social Networks such as Picasa, last F.M., and YouTube, provided users with a new way of publishing media and socializing online. This era of online social networking saw the creation of numerous unique services. For example, in 2003 a site named couchsurfing.com was published. Couchsurfing.com was truly unique in that it allowed users to form profiles with the aim of spending the night at random people's homes. This is actually a service that has grown exponentially. Many younger individuals have used couchsurfing.com to travel around Europe and explore new cities.

The mainstream online social networks of today began to emerge In 2006. On July 12th 2006, an article in Marketing Vox stated that "MySpace.com has surpassed internet



powerhouses Yahoo Mail and Google as the most popular U.S. website" (para. 4). During this time period MySpace visits accounted for an amazing "4.5% of all U.S> internet visits" ("MySpace surpasses Yahoo Mail, Google in Popularity," para. 2). Many people believed that MySpace was successful because it let "its users do what they want" (Larry Weber, p.139). For many years, most people believed that MySpace would become the main online social network just as Microsoft Windows had become the main operating system years earlier. However, in late 2007 an online social network by the name of Facebook overtook MySpace in terms of average daily visitors.

Before the success of Facebook, it was generally understood that the model for a successful online social network was based on a site's quantity of applications and the extent of its user's control. However, Facebook found success with significantly less user control. Instead of focusing on the quantity of self expression applications, Facebook realized that the most important thing was making applications easier to use. The Facebook model showed that application usability is just as important as application capacity.

Prominent online social networks like Facebook and MySpace are dependent on the content that their users publish. Even more important than application usability or capacity are user participation and new member acquisition. Although it can be difficult to draw concrete conclusions about complex systems like online social networks, it is safe to say that they can only survive by collecting copious amounts of private data.

THE PERMANENCE OF THE INTERNET

Online social networks are seemingly inseparable from the internet. Just as law can't be understood without politics online social networks can't be understood without the internet. In order to use an online social network one must use the internet. Thus any factor that affects the internet will likely affect the users of online social networks as well. Furthermore any legislation, judicial precedent, or practical reality that impacts the internet will also impact the users of online social networks.

This section of the paper will explore how the internet is becoming a permanent system. Political, economic, and institutional factors have lead to the creation of permanent internet archives. These internet archives can be detrimental to online social network users who have personal or detrimental information posted on the internet. This paper does not view permanence like the atom which persists throughout all time. Instead, this study believes that the files on the internet will endure like the ink from a permanent marker. They will most likely survive until the unforeseen future or the end of their relevance. This means that the actions of online social network users will survive until the unforeseen future as well.

What is Permanence?

Absolute permanence is a long debated topic. Countless hours of theological, philosophical, and physical examinations have been invested in debating the existence of absolute permanence. Many have suggested that “as for absolute permanence, we know

this even less in the field of human experience, than in the case of chemical elements." ("Journal of Philosophy," p.375) This rational is widely accepted by many scientists and theologians. This concept explains that while most objects are destroyed the essence or matter that makes up its existence survives forever. The infamous Buddhist and Yoga scholar Patańjali once wrote he "had to admit the absolute permanence of matter." The philosopher Immanuel Kant theorized that the permanent nature of matter allows the sequential events of life to unfold and take place. Kant states that "solely through the permanent does sequential exist." (Journal of Philosophy, p.254)

Regardless of their position most individuals can agree on several principals related to absolute permanence. It is generally accepted that if absolute permanence exists then its occurrence is rare. Second permanence relates to objects, systems, and concepts in different ways. For example, the permanence of an atom would be entirely different then the permanence of the physical laws of matter.

One should also accept that the concept of permanence is often used in a relative context. Furthermore, this relative context can be affected by ones concept of existence. If a logical person is to believe that something is permanent then that person must perceive that nothing can or will cause that thing to stop existing. Most people believe that when a good and moral person dies they continue to exist as a spirit. Similarly, many scientists believe that after an object is destroyed it continues to exist as matter. These examples indicate that one's definition of existence creates a relative context for their perception of permanence. Ones acceptance of permanence is relative to their perception of existence.

The word permanent is most commonly used in a relative and practical context. The word is generally used to describe a situation of unforeseeable change. Many people are

referred to as being permanently disabled even though it is obvious that they won't be disabled in a million years.

The word permanence is commonly used to describe the various degrees of sustainable, perpetual, and undeviating situations. For example, In Mary Wollstonecraft's famous *Vindication of the Rights of Woman* she writes that the bond between parent and child is permanent. However, she explains that this bond is a "much more permanent connection than love between married people."(p.121) In this instance Wollstonecraft uses the term permanent to describe a situation's quantity of existence and its likelihood of perpetuation.

This paper addresses the permanence of a system. Most scientists view perpetual systems as cyclical systems. Scientists view these cyclical systems in terms of inflow and outflow. It has been said that a systems continued existence is dependent on the "permanence of certain components of the system, in particular those which control the inflow and outflow." (Journal of Philosophy, p.594) In order for a system to be permanent it must be able to acquire as much inflow as outflow. A system's degree of permanence is generally based on its likelihood of perpetuation. If a system is more likely to survive then it is often referred to as being more permanent.

This study utilizes a relative and practical approach in defining perpetual systems. It is believed that a permanent system is one in which its outflow will be recouped by its inflow for the unforeseeable. It is also believed that permanence is related to historical significance. A permanent system is sustainable. A sustainable system is one which has the capacity to last as long as it's natural environment. A system is permanent if it has the means, motive, and likelihood, of unforeseeable survival.

Monetary Incentives for Data Acquisition

Current economic factors are a central cause of the recent expansion in data acquisition. Storing data is cheap while possessing data is valuable. Internet data is free, unrestricted, and amongst the most valuable. These economic factors provide the means, motive, and likelihood of increased data acquisition and the permanent storage of internet data.

Every file on the internet can be documented and permanently stored. This capability not only exists, but is growing all of the time. Data storage is getting cheaper and easier each and every day. Furthermore, the collection and storage of data allows technicians to construct massive data archives. Technicians primarily collect data from the internet because its unrestricted acquisition allows for the creation of large data archives.

Data archives have proven to be extremely lucrative for companies like Google, MySpace, and compete.com. It has been said that "all data can be converted to monetary value." (Phillips, "Converting Data") Most economists believe that advances in data synthesis will make information even more valuable. Many statistical researchers argue that "data collection can be even more valuable than research" (Cohen, White, and Rust, p.93). As the value of information increases the demand for data acquisition will likely grow as well.

If one accepts Adam Smith's principal of capitalistic markets then one would assume that the demand for information will ultimately drive suppliers to acquire new data and store older data for longer periods of time. Therefore, easily acquisitioned data such as the internet will more likely be captured and more likely to be stored in a permanent manner.

Internet Archives and the Wayback Machine

Many people think of the internet as a system that stores data temporarily. The internet is a place where one can post files and delete files. Many people think that deleting files from the internet is the same as deleting files from a computer. They assume that the deletion an online document permanently removes that document from the internet. In reality, this assumption is often false. In the book, *The lawyer's guide to fact finding on the Internet* Carole A. Levitt, Mark E. Rosch, and the American Bar Association (ABA), state that "just because information has been removed from a site does not mean that it is gone forever" (p.136).

The ABA's book claims that a program named The Wayback Machine can help individuals retrieve data that has been removed from the internet. The Wayback Machine is essentially a large data storage device. The Wayback Machine uses its storage capacity to collect and store hundreds of terabytes worth of internet data. The machine copies and stores WebPages, music, and data, from all over the internet. The Wayback Machine then catalogs this data in chronological Internet Archives. By searching through internet archives, individuals can retrieve files that have been deleted from the internet.

The project's intention is to take chronological snapshots of the entire internet. Advocates claim that the Wayback Machine is the best way to preserve and document humanities most significant virtual accomplishment, the internet.

The Internet Archives allows individuals to view the chronological changes to websites. With the Wayback Machine one can see how websites like Google and Facebook have changed overtime. The ABA states that if one used the Wayback Machine to visit the

"For Lawyers web site as it appeared in May of 2000, you would be able to click through all the various pages then available" (p.137).

In order to capture and document something as large as the internet a system one needs special software. One of the best tools for data archiving is a crawler. Most Americans are familiar with popular web crawlers like Yahoo and Google. However, the Wayback Machine's crawler is more thorough than average crawlers. According to Patrick Panoz, the "crawler" that captures websites for the Wayback Machine has been "incorporated into both Netscape Navigator and Microsoft Internet Explorer as part of their smart browsing" (para.7).

Panoz also explains that "the Internet Archive's automatic system has crawled the Internet every few months since 1996, and has taken the equivalent of electronic snapshots of the entire Web." (para.7) In order to store this mass compellation of websites, the Internet Archive has become the world's largest database. In fact, the Internet Archive eclipses "the amount of data contained in all the libraries of the world" (Panozk para.8)

Data Collection and National Security

For future states, the internet security will increasingly be seen as a matter of national security. For numerous reasons it is in the best interest of the state and its citizens to collect, monitor, and document the files that make up the internet. In the book *National Security,* Hsinchun Chen and Daniel Zeng describe how the U.S. performs various forms of "Eb structural analysis," (p.248) "hyperlink analysis," (p.250) and "Web Harvesting." (p.251) These techniques illustrate that modern nations use data acquisition and analysis for National Security purposes. Through internet archiving techniques such as web

harvesting the government can collect valuable information, track criminal actions, and more accurately evaluate issues of national security.

Governmental Avocation of Data Acquisition

In recent years, governments such as Australia and the U.S. have begun to publicly advocate the internet archiving and web harvesting. The support of such techniques is primarily related to issues of domestic and national security. According to Margaret Phillips the Director of Digital Archiving at the National Library of Australia, the Australian government has ordered that its national library "harvests Australian online publications for inclusion in PANDORA, Australia's Web Archive."(para.8)

In November of 2001 Mark Richard from the Criminal Division of the United States Department of Justice described America's position data retention to the European Union's Forum on Cybercrime. In this speech Richard explains that we currently live" in a world where terrorists" ... "are not confined by national borders or geography" (p.1, para.4) In Richard's opinion the events of 9/11 are evidence that terrorists are capable, willing, and determined to use technology systems in their efforts to promote global terrorism. Richard also states that "access to historic computer traffic data, such as connection logs, in conformity with accepted due process protections is particularly critical for investigators to identify terrorists."(para.5) The need for data retention through archived collection is also applicable to the private sector efforts to alleviate crime and fraudulent behavior. Because archive data is critical to the apprehension and prevention of criminal and terrorist acts, the U.S. adamantly "opposes mandatory data destruction regimes." (para.6) It is articulated that destroying valuable data could

“impede criminal investigations and ultimately diminish public safety". This opposition to legislated data destruction is America's official international data retention policy.

Governmental Requirement of Data Archival

In recent years, governments have gone beyond avocation and have even begun to require the retention of specific private data. In the book, *Access denied: the practice and policy of global Internet filtering*, Ronald Deibert, John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain describe that the European Data Retention Directive requires European internet service providers to "retain specific data pertaining to communications - in particular, with regard to internet access, e-mail, and telephony.” (p. 193)

Legislative efforts to mandate data retention in the U.S. have been implemented in a unique manner. European legislation requires Internet Service Providers to retain internet data. U.S. legislation requires Internet Service Providers to retain the data trail of individuals. Instead of focusing on internet data, U.S. legislation has focused on internet users. U.S. legislation requires that data uploaded, downloaded, or viewed, by internet users be recorded.

HR107c Section 2703 of title 18, United States Code states that “a provider of an electronic communication service or remote computing service shall retain for a period of at least two years all records or other information pertaining to the identity of a user of a temporarily assigned network address the service assigns to that user." (section 5)

It should be noted that the language in HR107c provides the government with considerable power. The term “temporarily assigned network address” (section 5) is of particular importance. The term refers to what is known as an internet protocol address or IP address. In order for an individual upload, download, or perform any task online a

user must obtain an IP address. For many years IP's have been used to trace and track internet users. Ironically IP addresses are the "same technology that serves up tailored banner advertisements." (Economist, p.22)

The bill's use of IP addresses provides dramatic power because it allows the government to construct comprehensive data trails. When one realizes that that every online action requires an IP and that every IP is required to be tracked, the true power of HR107 becomes apparent. Furthermore, HR107 requires that "all records" (section 5) be saved for "at least" (section 5) two years. Such wording does not inhibit the government from retaining data longer the 2 years. This bill not only allows but requires that every file published, seen, or saved by an American must be documented, saved, and stored.

Data storage will likely continue to decrease in price. The practice of internet archiving will continue to increase as new and affordable applications for mass data are discovered. Furthermore, financial, legal, and security objectives will dictate a continual expansive evolution in internet archive systems. Currently, there are no laws that significantly restrict the collection of private internet data. Even if strict U.S. laws were established, the internet is an international phenomenon that doesn't fall under any government's jurisdiction. Therefore, it is likely that new and even more comprehensive internet archives will continue to emerge and permanently record massive amounts of private data.

A system is considered permanent if it has the capacity to endure until the unforeseeable future. The systems of internet archiving, data retention and data mining are all such systems. Monetary, security, and political forces will perpetuate these

systems into the unforeseeable future. While not every file posted to the internet will be saved; most will, and all can be.

The internet is an abstract concept which is generally perceived as a network that connects devices and links data. The extent of the internet is currently unclear. Is any system that provides data connectivity on a global scale considered an internet? While this question is invaluable it is also irrelevant. Regardless of what it is called or referred to, systems that connect, store, and catalog data will exist for the unforeseeable future. Adept critics will note that a cataclysmic catastrophe could destroy the internet and technology as a whole. However, such a critique uses possibility instead of probability. Other critics might note that theories such as Edwin Hubble's Universal Expansion and Paul Dirac's antimatter reveal that even matter and the universe are not permanent. Such a concept of permanent is not what is intended in this paper. Instead, it is believed that the internet holds elements of permanence because it is a system that has the capacity and likelihood to endure until the unforeseeable future.

Today alone, the online actions of every American will be documented and stored; millions of children will submit personal information to online social networks, and thousands of adolescents will publicly post defamatory pictures that they cannot delete. If files posted to the internet are permanently stored then information posted through online social networks will permanently stored as well. Online social networks depend on their user's submission of personal data. If this data is detrimental then the unforeseeable perpetuation of such data could cause extensive harm.

Internet archiving began long before online social networks ever existed. In fact, in the internet's infancy dangers related to internet archiving were minimal. The danger of data

retention and internet archiving dramatically increased as online social networks became prominent. Before chat rooms, blogs, and Facebook, few people posted personal information on the internet. As the popularity and prominence of online social networks grew the people's inhibition for posting private data seemed to deteriorate.

One of the most negative societal effects of online social networking is due to unawareness on the part of the user. The majority of online social network users have no clue that the information that they post can be permanently stored. Yet legislation like HR 107c requires that the posts of every American online social network user is documented, saved, and stored. If someone with wrongful intensions were able to obtain the data derived from HR 107c, the negative societal effects would be unimaginable. It is believed that if more people were aware of the permanent factors related to the internet that they would be more careful and thus better protected when using online social networks.

POLITICS AND ONLINE SOCIAL NETWORK LEGISLATION

One of the easiest ways to model political environments is by examining legislative opposition and avocation. Analysis of prominent legislation allows one to better understand the political dynamics which govern partisan organizations and individual legislators. Modern societies often tend to use legislation as a way of mitigating negative societal effects. If online social networks have negative effects then the best way to eliminate such effects is through proficient legislation.

In America the creation of legislation is dependent on politicians, partisan organizations, and bureaucratic institutions. The relationship between, among, and around these entities is often referred to as politics. A politician's ability to implement legislation is derived from her mastery of the political system. Therefore, if one desired to ameliorate the negative effects of online social networking through legislation then an understanding and aptitude for politics would be highly desirable.

Currently the most prominent legislative controversy about online social networks has involved the use of such networks in public institutions. This controversy surrounds partisan legislation which seeks to use bureaucratic regulation to restrict the use of online social networks. At the forefront of this conflict there have been two important federal legislators, Democratic U.S. House of Representatives member Bart Stupak and Republican member Michael G. Fitzpatrick. By introducing the Deleting Online Predators Act (DOPA), congressman Fitzpatrick presented one of the first pieces of legislation aimed at combating the negative effects of online social networking.

Deleting Online Predators Act

The summary to the Deleting Online Predators act states:

"Deleting Online Predators Act of 2007 - Amends the Communications Act of 1934 to require schools and libraries that receive universal service support to enforce a policy that: (1) prohibits access to a commercial social networking website or chat room unless used for an educational purpose with adult supervision; and (2) protects against access to visual depictions that are obscene, child pornography, or harmful to minors. Allows an administrator, supervisor, or other authorized person to disable such a technology protection measure during use by an adult, or by minors with adult supervision, to enable access for educational purposes. Directs the Federal Trade Commission (FTC) to: (1) issue a consumer alert regarding use of the Internet by child predators and the potential dangers to children because of such use, including the potential dangers of commercial social networking websites and chat rooms; and (2) establish a website resource of information for parents, teachers, school administrators, and others regarding potential dangers posed by the use of the Internet by children" (1)

Benefits of DOPA

There are many benefits relating to congressmen Fitzpatrick's DOPA. Perhaps the most significant aspect of DOPA is its goal of protecting children from the dangers of online social networking. The bill's proposal highlights the significance of the issue. Roman Espejo states that "in July 2007, social networking service MySpace identified and removed twenty-nine thousand known sex offenders' profiles from its website." (Espejo

7) To makes matters worse, MySpace acknowledges that they do not have the capacity to remove sex offenders who use “false identities.” (Espejo 7)

Another benefit of the DOPA bill is that it provides a good definition for online social networks. The bill explains that a “website could be defined as a social networking service if it: is offered by a commercial entity; permits registered users to create an online profile that includes detailed personal information; permits registered users to create an online journal and share such a journal with other users; elicits highly personalized information from its users; and enables communication among users.” (Espejo 7) This definition is suitable because it is descriptive and dynamic. The lengthy and descriptive wording provides insight that could help individuals identify unique online social networks. The definition's ability to use one or more of the mentioned criteria provides flexibility. Through this bill any system that “enables communication among users” (Espejo 7) could be considered an online social network.

The bill's flexibility can be seen in one of its restrictions. Section three of DOPA states that the bill's ban on online social networks can be suspended “by an adult or by minors with adult supervision.” (Fitzpatrick) This legislative caveat provides DOPA with the flexibility to accommodate different individuals and different situations.

Negative Attributes of DOPA

Unfortunately some of DOPA’s language provides discrepancies between the bills legislative capacity and its stated goals. The uppermost goal of the legislation is the protection of children from predators who use online social networks. However, the bill attempts to carry out this goal in a way that neglects the actions of individuals.

As it has been explained, the proposed legislation does not pertain to the misguided actions of children or the heinous actions of online predators. In many ways the legislation's inability to address and reduce the negative actions of individuals goes against the bill's primary goal. If a bill does not pertain to the actions of individuals then such legislation cannot fulfill the goal of protecting children from predacious actions. One of the most important inadequacies of the bill is its inability to address the actions of predators that are technologically knowledgeable. It is not unreasonable to assume that there are many predators who posses sufficient knowledge to bypass online restrictions. The bill's inability to restrict, reduce, or address the actions of such predators is unacceptable.

Unfortunately, DOPA also fails at inhibiting children from intentionally or unintentionally putting themselves at risk online. Through intentional or unintentional actions children can potentially bypass the proposed internet restrictions and gain access to online social networks.

Many people do not realize that they can bypass software restrictions inadvertently. One classic example of this principal could be seen on the login page of Windows 98. In order to login users were required to enter the appropriate username and password. Many users of Windows 98 inadvertently came to realize that pressing *Cancel* instead of *Ok* allows the program to disregard the password requirement. Although it was often used intentionally, the Windows 98 *Cancel* button is a good example of how novice computer users can unintentionally bypass software restrictions.

In the book "How to Do Everything with Google," Fritz Schneider explains search engines like Google have made unparalleled bodies of information at the fingertips of

humanity. But, it is important to realize that this information is available to almost all age groups. This means that intelligent children can find the information to overcome significant parental restrictions.

After typing the words “how to break parental control” into Google, the first link that is generated is titled *How do I break through parental control?* The page states that “for a computer you can set it into safe mode on start up by holding *Shift*, however if you do that you cannot access outside information packets, i.e. the internet which is what I assume you are looking to do while they are gone. However once in safe mode you should be able to access the administrator tools and disable any restrictions.” (Erik Stenny) These are easy, descriptive, and accurate directions, for disabling some of the most powerful Windows-based parental controls.

Earlier in the paper the popularity of online social networks was explained. The information shows that online social networks are among the most popular internet trends. By enacting the DOPA, children would be restricted from using one of today’s most popular social experiences. This deprivation will likely encourage students to find ways around restrictions. The availability of information will make effective parental restriction all the more difficult.

The most prominent opponent of the DOPA has been Democratic congressman Bart Stupak. Stupak opposes the bill because it uses “broad language” (Stupak 1) and “does not address the problem of online child exploitation.” (Stupak 1) On July 26, 2006 Stupak provided oppositional speech about DOPA to the US House of Representatives. Stupak began his speech by stating that the DOPA “bill will not delete online predators. Rather, it will delete legitimate web content from schools and libraries.” (Stupak 2) It is

important to note that the bill contains no language that allows or provides for the deletion of “legitimate web content,” (Stupak 2) However; Stupak’s opening argument does highlight a fundamental inadequacy in the DOPA.

Stupak’s opening argument is correct in that the DOPA “will not delete online predators.” (Stupak 2) The bill doesn’t allow government agencies to delete an individual’s web content. The bill merely orders schools and libraries to monitor and prevent access to online social networks. The bill is not meant to delete predators. Rather, the bill is an attempt to protect children in schools and libraries from online predators." (Stupak 2) The complete disconnect between the DOPA’s title and purpose is one of its most obvious negative aspects.

Stupak also argues that the proposed legislation is irrelevant. According to Stupak, current laws render DOPA’s legislative accomplishments mute. He states that “there is already law on the books that requires schools and libraries who receive e-rate funding to monitor children’s internet use and to employ technology blocking children or preventing children from viewing obscene and harmful continent.” (Stupak 2) At first glance it can be hard to identify the differences between DOPA and the current law the Stupak mentions. The difference is that the current law does not address online social networks.

Stupak’s primary point of opposition was that DOPA ignores “the real threat to our children.” (Stupak 3) DOPA is seen by Stupak as a bill that does not go far enough to protect children from online exploitation. On page three, Stupak states that DOPA “does not address the real issue of educating children about the dangers of the internet.” It is possible that Stupak’s proposal of education and awareness might deincentivize children from being reckless on the internet.

Stupak even claims that DOPA would act contrary to its goals and place children in more danger. Stupak states that in a “hearing from 38 witnesses on the issue, there was not one mention of online child exploitation being a problem at schools or libraries.” (Stupak 2) Stupak explains that the “real threat lies in children using these sights in their rooms without adult supervision.” (Stupak 3) It is the belief of Stupak that children are most vulnerable in the home and not at the schools. By disallowing students from using online social networks in schools “will actually drive children to go to unsupervised places, unsupervised sites.” (Stupak 3) In conclusion, Stupak states that if DOPA is passed children will “become more venerable to child predators."

DOPA does not discourage adolescents from ignorantly posting private information on online social networks. It doesn’t promote childhood awareness about the dangers of online social networking or start an initiative to identify sex offenders and actually delete them. Instead, it requires federally funded schools and libraries to enforce “a policy of Internet safety for minors that includes monitoring the online activities of minors.” (Section 3, Fitzpatrick) Although DOPA’s indirect institutionalized approach of regulating online social networks might have many benefits, its method has significant faults.

The Congressional Debate of July 26, 2006

Analysis of House floor rhetoric indicates that DOPA was a highly partisan bill. Throughout the 4 sessions of debate none of the six Republican speakers voiced opposition for the bill. Furthermore, out of the six Democratic speakers only Sheila

Jackson supported the bill. Stupak was even quoted as saying that he was “disappointed that this issue" had become "a partisan issue.” (3)

On July 26, 2006, numerous Democrats blasted the bill. In the forth session of deliberation, Congressmen Markey, Dingell, Inslee, Watson, and Stupak spoke about DOPA.

Edward Markey was the first Democratic Congressmen to speak at the July 26th congressional debate. Markey began by stating that he was in “support of this legislation.” (Section 41) Despite his initial statement Markey spent most of the speech discussing the failures of DOPA.

Markey dislikes the language in the DOPA bill. According to Markey DOPA’s language “remains overbroad and ambiguous.” Markey also disagrees with DOPA’s funding mechanism. DOPA uses public funds as a way of enforcing the act. Markey feels that using public funds as a mechanism for limiting liberty goes against the principals of public finance. Markey also asks, “Why should these requirements only apply in schools receiving e-rate funding?” Shouldn’t the initiatives of DOPA be implemented through public law?

Markey argued that DOPA would be ineffective at accomplishing its purported goals. Markey states that “the Attorney General from Texas, for example, testified that just going after schools and libraries wouldn't achieve a whole lot.” (Section 41) Markey shares in Stupak’s opinion that the bill's title is misleading. In his speech, Markey exclaimed that “If the goal is to address the issue of online predators, this bill proposes an ineffectual remedy.” (Section 41)

During the debate congresswoman Watson opposed DOPA on the grounds that it “would curb Internet usage as a means to protect children.” (Watson Section 41)

Like many of the other Democrats Watson prefers to use education instead of force when combating online predation. Watson said “rather than restricting Internet usage, parents, teachers, and librarians need to teach children how to use our ever changing technology.” (Section 41) Watson thinks that federal funding of internet education would be more effective then “additional administrative tasks” (Section 41)

Watson also agrees with her fellow Democratic congress persons in that funding mechanisms are not the best way to protect children. Like Markey, Congresswoman Watson feels that all children are entitled to protection from online predators. Watson stated that children would be better protected by fully funding “police departments across the Nation to monitor online predators.” (Watson section 41)

Watson concluded her speech by stating that “bill of this magnitude will send us down the slippery slope of legislating even more Web sites and infringing on our right to information.”

Another prominent speech against DOPA was provided by Democrat Jay Inslee. Inslee described DOPA as inferior, substandard, and ineffective legislation. Inslee even questions the motives behind DOPA by stating that the bill has been advocated because it is,” in effect, a good press release, but it is not effective legislation addressing a huge problem threatening our children.” (Section 41)

Inslee doesn’t believe that the bill would provide children with any protection from online predators. According to Inslee, “only 10 percent of the abused kids are online and hardly any of them from schools.” Since DOPA would only effect this “infinitesimal

portion” (Section 41, Inslee) of children. Inslee believed that DOPA was ineffective. Inslee even states that “this legislation would not save one single child one single time.” (Section 41)

The final oppositional speaker was Democrat John Dingell. In reference to online predators, Dingell states that “every right-thinking and decent American opposes this practice.” (Section 41) However, Dingell believes that DOPA would not be the most effective means of remedying the practice.

Congressman Dingell agrees with Stupak, Inslee, and Markey that in schools and libraries are poor places to combat online predators. Current law and statistical realities show that these areas are among the most secure.

Perhaps the Dingell’s most interesting statement was his belief that the bill was more about politics than effective governance. He states, “I can't tell whether it is a bunch of Republicans who are panicky about the next election or whether it is a situation in which everybody is trying to rush to get out of town to go on an August vacation.” (Section 41) Dingell explains that the bill was rushed through Congress so fast that its true affects were not thoroughly understood. Dingell believed that certain aspects of the bill such as its title and its rate of legislative progression carry a “curious smell of partisanship and panic.” (Section 41) In conclusion, Dingell states that he suspects that DOPA’s true purpose has been to "help some of my panicky Republican colleagues save themselves in a difficult election."

In the end, the other GOP members responded to the Democrat’s attacks by restating the same points that Fitzgerald had already made. They emphasized the importance of protecting children and provided statistics relating to Internet predators. The Republicans

had a difficult time explaining how the bill would delete predators, and protect children at home.

Based on the debate, many would assume that the strong arguments of the Democrats would bring a vote against DOPA. Instead the bill was passed by an immense majority. The bills success can be explained by several political factors. Firstly, the bill’s success was primarily due to Republican's large majority. It should also be noted, voting against bills with names like DOPA does not look good on a politician’s record. It all boils down to politics.

PUBLIC PRIVACY AND ONLINE SOCIAL NETWORKS

Do Americans have the Right to Privacy?

Privacy is one's freedom to keep, maintain, and deny the submission of personal information. “Privacy can mean keeping information to ourselves. It can also mean being left alone at times, and being free from others interfering in our lives.” (Garrett 6) Garret's definition describes privacy as a conditional situation. This definition provides a philosophical interpretation of the concept of privacy. Famed political scientist, Adam Carlyle Breckenridge views the concept of privacy as a right. Breckenridge states that privacy “is the rightful claim of the individual to determine the extent to which he wishes to share himself with others” (1)

The right of privacy has long been debated in American politics. It is important to note that “privacy is never mentioned in the US Constitution” (Garrett 74). In fact, “the first case to recognize a constitutional right to privacy was the famous case of Griswold v. Connecticut, decided in 1965” (Garrett 74).

Griswold v. Connecticut is most prominent precedent for one's constitutional right to privacy. The majority opinion Supreme Court Justice wrote that the “Bill of Rights have penumbras, formed by emanations” which provide for ones right to privacy” (1). In a concurring opinion, Justice Goldberg explained that the right to privacy was most strongly asserted in the 9th Amendment to the constitution. The 9th Amendment states “The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people” (US Constitution). Goldberg wrote that the

constitution's description of "rights could not be sufficiently broad to cover all essential rights" and that such rights were instead protected by the elasticity of the 9th Amendment. In an additional concurring opinion, Justice White and Justice Harland asserted that the right to privacy is provided by the due process clause in 14th Amendment.

Some have argued that the 4th Amendment guarantees one's right to privacy. The amendment provides "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The use of the 4th Amendment is most prominent in the Supreme Court case *Miranda v. Arizona*. The case established that governmental invasions into private property are only acceptable when a person is aware that such an invasion will occur. Garret explains that the 4th Amendment requires the person who is being searched to be told" (15).

Others, like Harry Brown, have argued that the 5th Amendment provides the right of privacy. Brown states that the right to privacy isn't specifically mentioned in the constitution, because the "Constitution isn't about what *people* can do; it's about what *government* can do." The 5th Amendment states that "powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people." Brown sternly asserts that no where in the constitution is the government provided the right to deny or invade ones privacy. Therefore, if a person does not live in a state that rejects one's right to privacy then that individual by default has the right to privacy.

HR107c and Its Abrogation of the Right to Privacy

HR107c requires internet service providers to record and document every American's internet history. After recording this data, the government is not constrained by any current law from reviewing such information. This law seems to violate almost every articulated protection of privacy. Nowhere in the Constitution is the government provided the right to mandate the documentation of personal data. Thus, the law violates Harry Brown's position on the 5th Amendment.

The 4th Amendment supposedly guarantees "people to be secured in their persons, houses, papers, and effects." But, wouldn't one's "effects" be insecure if the government required the documentation of their internet history? Furthermore, wouldn't HR107 violate *Miranda v. Arizona's* interpretation of the 4th Amendment in that it allows government officials to digitally search an individual without their knowledge?

The 9th Amendment explains that the governments constitutionally provided rights "shall not be construed to deny or disparage others retained by the people." Government officials argue that HR107c is constitutional, because it falls under the government's authority to provide national security. However, the government's attempt to provide national security through HR 107c has been "construed to deny or disparage" the right to privacy.

Rights have generally been created for the purpose of protecting societal liberty. The right of privacy has one of the longest histories of judicial deliberation. The right of privacy's long history provides a comprehensive analysis of its benefits, determents, and effects on society. Throughout right of privacy's immense judicial history it has been

repetitively asserted that the neglect of one's right privacy is detrimental to society. It follows that a violation of one's right to privacy can also be detrimental to society. HR107c is a blatant abrogation of one's constitutionally provided right to privacy. The expansion in use of online social networks has equated with an increase in the amount of personal information posted online. Through HR107c, the government has the ability to record, document, and search through all such information. Therefore, the increase in online social networking has resulted in an increase in the government's acquisition personal data and an increase in the government's invasion of public's privacy. If one accepts the notion that increased violations of privacy are detrimental to society, then one would also accept that an increase in online social networking can have negative social effects.

The Public Figure

The concept of a public figure is important when discussing one's right to privacy. This is because public figures are largely exempt from privacy protection. Smith writes "those who publish otherwise libelous statements about public figures are usually protected" (Smith 31) One might notice that Smith specifically addresses libel and not privacy law. In fact, the public figure doctrine is derived from tort law that only pertains to libel. However, much of privacy law has been modeled after much of the older libel laws. However, in cases of "private facts, courts often borrow the public figure doctrine from the law of libel," (Smith 31)

The public figure doctrine has also been addressed in the court system. The case *New York v. Sullivan* was the first Supreme Court case to draw the "distinction between

public and private persons." (Scheppele 214) However, Sullivan did not address all issues of public privacy. The clearest revocation of a public figure's right to privacy came in the case *Estill v. Hearst Publishing Company*. In the regards to the right of privacy "public figures are generally considered to have waved most of their right to privacy." (Scheppele 214)

What is a Public Figure?

Upon coming to the realization that public figures have no sufficient right to privacy, it is only natural to ask, who is a public figure. Unfortunately, "the definition of public figures is somewhat vague". (Einsohn 417) It seems that "the definition of a public figure has changed with the makeup of the Supreme Court." (Davidson 155)

There are several provisions that pertain to public figures that are generally accepted. In the Supreme Court case *Gertz v. Justice Powell* states that a public figure is one who has attained "general fame or notoriety in the community." (Gertz) The case also established that if a person "voluntarily injects himself or is drawn into a particular public controversy" (Gertz) they can become a public figure. The case *Varian Medical Systems Incorporated v. Delfino* states that a person can become a public figure if they "advertise or sell to the general public." ("Delfino") In the Delfino case, it is further asserted that a person can be a public figure if they have a "pervasive influence in the community."

This paper holds that invasions of privacy can have negative effects on society. As it has been stated, if a person is considered or defined as a public figure then that person is generally understood to have no right of privacy. In exploring the definition of public figure it is shown that the term is vague, unclear, and inadequately defined. In general,

courts have come to judge the existence of public figures on a case by case basis. The ambiguity in this term's legal definition is startling.

From Private Citizen to Public Figure

The profiles have made members of online social networking websites public figures to some degree. In fact, it's becoming hard to differentiate between a 7 year old YouTube user and a person with "general fame or notoriety in the community." ("Gertz") Furthermore, Facebook provides millions of users with the ability to voluntarily join massive groups, follow popular causes, and advocate, oppose, or interject on matters of "particular public controversy." (Gertz) The unique nature of online social networks makes the term public figure even harder to define. If one accepts the current legal definition of public figure then it is hard to argue that online social networks have not brought millions of people from private citizens to public figures.

One of YouTube most prominent videos is of a 7-year old boy named David. The video was recorded after David's visit to a dentist. During the dentist appointment, David received a powerful drug called laughing gas. The video portrays David in a euphoric, estranged, and terrified state. At one point David even asks his father if the feeling is going to last forever. Needless to say, the video is not a great depiction of David's best attributes.

In regards to this paper, David's psychological state is of minimal importance. David's video is important because it had been viewed 37,728,360 times as of December 2009 and 49,598,689 times as of January 19, 2010.. That's 22 million more visitors than Texas has people. On David's YouTube page there is also a link to a website which is solely devoted to the video. His YouTube page even has a link that allows visitors to purchase

T-shirts and merchandise. Based on current legal definitions, David's profound fame almost certainly qualifies him as public figure. Therefore, David's trip to the dentist might revoke his right to privacy. It is amazing to believe that an online social network like YouTube can provide a legal means of revoking a 7 year olds' right to privacy.

One of Facebook's most popular functions is its Causes application. The program allows individual to create causes and raise money for charitable organizations. The application is truly remarkable. Through the actions on individual Facebook users, the application derived $14,278 in the week this paragraph was written. The program also highlights the top earners of each week. One of the top earners was Sean Parker. In one week Sean raised $19,340 for *Malaria No More*.

Unfortunately, the Causes application can turn altruistic acts into a revocation of rights. Not only can the Causes page raise an individual to unintentional fame, but the application can also encourage users to engage in issues of "public controversy." (Gertz) For example, the application allows individuals to publically endorse controversial causes such as the *New York Abortion Access Fund.* The Causes application clearly demonstrates the need for a better definition of public figure. Current legislation and judicial precedent could revoke one's right to privacy, because of their involvement in an altruistic cause.

Based on the current legal definitions, online social networks are converting private citizens into public figures at an alarming rate. Despite their intention online social networks could be eliminating the right of privacy for millions of Americans. If one views the elimination of privacy rights as detrimental then, online social networks can most certainly be seen as contributing to negative societal effects.

As online social networks grow, their user's submission of personal data grows as well. As the submission of personal data grows, the quantity of personal data in internet archives grows as well. Increases in the submission of private data onto public networks will also increase the number of public figures. An increase in the number of public figures will ultimately decrease the number of individuals who have the right to privacy. Therefore, there is an inverse relationship between online social networks and the right to privacy in America.

The inverse relationship between online social networks and the right to privacy in America is entirely dependent on the public figure doctrine. Without the public figure doctrine, an inverse relationship between online social networks and privacy would be much less clear. It is the position of this paper that the current relationship between these two entities can cause negative effects on society. In order to remedy the current paradigm, this paper makes two propositions:

First, legislators, politicians, or judges could remedy the situation by establishing a better legal definition for the term public figure.

Second, the situation could be remedied by elimination the public figure doctrine. Perhaps, even public figures deserve some forms of privacy.

CASE STUDY

Methodology

This case study examines whether online social networking facilitates the infringement of one's "Right of Publicity" (Winn & Wright, 2002, 1) and/or one's ability to refuse "Public Disclosure of (their) Private Facts." Anything that is conducive or influential to a violation of either of these tort laws is considered by this paper to be a contribution towards infringement. This study is not narrowly focused on determining whether websites such as Facebook and MySpace are violating privacy laws. Instead, this study will determine whether online social networking contributes to infringements of privacy law committed by either the members or the owners of online social networking websites.

Public Disclosure of Private Facts

One law that can contribute to establishing an invasion of privacy is “Public Disclosure of Private Facts" (Scott, 2006, para. 1). According to Michael D. Scott in 2006, author of *Treatise, Scott-Information-Technology, §16.06C “Public Disclosure of Private Facts”*:

"An action for the public disclosure of private facts can arise when true, but confidential and highly offensive, facts about a person are made public. To establish liability for the publication of private facts, the following elements must exist:

1. There are private facts;

2. The facts are not related to an issue of public concern;

3. The facts were publicized; and

4. The publication was in a highly offensive manner.[84]

Facts that are already known to the public or are not offensive cannot be the basis for an action involving this doctrine." For example, publishing a person's name or address (absent any extenuating circumstances) or matters involving facts contained in public records, such as birth certificates, court records, or military records, are not actionable.[84.1] Under this doctrine, the disclosure must be offensive to a reasonable person. Further, the protection of private facts is not absolute and must yield if there is a strong public interest involved."

Peering beyond all the legal jargon, a "Public Disclosure of 'Private Facts" occurs when someone with privileged information publishes that information in a way that intentionally hurts another individual. For example, if a person betrays a friend by publishing hurtful information that was disclosed to him in private, it could be considered a "Public Disclosure of Private Facts."

It can be argued that websites like MySpace and Facebook contribute to the infringement of laws such as "Public Disclosure of Private Facts" (Scott, 2006, 1) because online social networking websites provide a medium through which individuals can publish hurtful information about others.

Due to section 230 in the Communications Decency Act of 1996, online social networking websites such as Facebook and MySpace are not responsible for the information that their members publish. The Communications Decency Act of 1996 states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." (Winn & Wright, 2002, para. 33) On February 13, 2007, the case of *Jane Doe and Julie Doe v. MySpace Inc. and News Corporation*, declared that websites like

Facebook and MySpace were "interactive computer services." Therefore, websites like Facebook and MySpace hold no legal responsibility for invasions of privacy committed by their users or members. In consequence, section 230 of the Communications Decency Act has been used in amalgamation with court cases such as *Jane Doe and Julie Doe V. MySpace Inc. and News Corporation* to argue that, websites such as Facebook and MySpace are not liable even if they provide a medium that facilitates or contributes to a "Public Disclosure of Private Facts." (Scott, 2006, para. 1)

Online social networking websites are not legally responsible for violations of "Public Disclosure of Private Facts" (Scott, 2006, para. 1) it is their members who hold the legal responsibility. If members of online social networks publish hurtful information about their friends, colleagues, or enemies, the member could be breaking the law. It is also important to note that many, if not most members, of social networking websites are unaware that publishing hurtful information can be illegal. Often times such members are naive and unaware that their online actions can be harmful to themselves as well as others. If laws like “Public Disclosure of Private Facts” (Scott, 2006, para. 1) are being broken, because of naive Online social network members, then it can be articulated that social networking is having a negative effect on society, because it is inadvertently contributing to individuals breaking the law. If members of social networking websites are aware that they are committing illegal actions, then it can be further articulated that online social networks are having a negative effect on society, because they are making it easier for their members to break the law.

Right of Publicity: Appropriation of Name or Likeness

According to the “Right of Publicity” (Winn & Wright, 2002, para. 1) individuals are entitled to the commercial value of their name and identity. One cannot use the name, picture, or resemblance of another unless that individual has granted permission. The *Treatise, Law-of-Electronic-Commerce, § 14.09 “Right of Publicity”* describes violators of the “Right of Publicity” (Winn & Wright, 2002, para. 1) as "any person who knowingly uses another's name, voice, signature, photograph, or likeness, in any manner, on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases of, products, merchandise, goods or services, without such person's prior consent, or, in the case of a minor, the prior consent of his parent or legal guardian, shall be liable for any damages sustained by the person or persons injured as a result thereof" (*Civil Code Section 3344-3346*, 2008, para. 1*).* For example, even if George W. Bush has publicly said that he likes Hershey's chocolate, the Hershey Company is not allowed to make an advertisement that uses George Bush's name, face, or likeness without his explicit permission.

In middle of 2007, Facebook implemented a new program called Beacon. One of the key aspects of the Beacon initiative was a concept called "social advertising." (*Leading Websites Offer Facebook Beacon for Social Distribution, 2007*, para. 1) Beacon creates social advertisements called "Facebook Ads" (*Facebook Unveils Facebook Ads*, 2007, para. 1) that use the names, faces, and personal interests of Facebook members for marketing and advertising purposes. If a Facebook member has indicated that he or she likes a particular product, then Beacon can be used to create personalized referrals which were to that member's virtual friends. These referrals can be misinterpreted as an

endorsement and even include personal pictures and information about members. The referrals turn Facebook members into personalized virtual spokespersons. According to Facebook's CEO Mark Zuckerberg, “Facebook Ads represent a completely new way of advertising online, combining social actions from your friends – such as a purchase of a product or review of a restaurant – with an advertiser’s message. This enables advertisers to deliver more tailored and relevant ads to Facebook users." (Zuckerberg, 2007, para. 2) Facebook is using its members "social actions" (Zuckerberg, 2007, para. 2) and information to make money from advertisers; such action appears to violate the “Right of Publicity” (Winn & Wright, 2002, para. 1) as defined by *Civil Code Section 3344-3346* in paragraph 10 of this paper.

Programs like Beacon show that online social networking websites like Facebook are using the names and pictures of their members for advertising purposes. Under the law “Right of Publicity” (Winn & Wright, 2002, para. 1), this action is strictly forbidden without prior consent. The evidence provided indicates that future cases involving social advertisements and the "Right of Publicity" (Winn & Wright, 2002, para. 1) are highly likely. In the online legal community the connection between social advertisements and “Right of Publicity” (Winn & Wright, 2002, para. 1) is already becoming prevalent. Recently the concept was discussed at great length on a Harvard website. On Harvard Law's website, William McGeveran J.D. made a comment that has received recent attention. McGeveran stated that social advertisements might be illegal, because "users are only asked in general if they want to share information, not if they want their name and picture to be featured in an ad for some product." (McGeveran, 2007, para. 5) McGeveran is referring to the fact that users are only aware that they have stated they like

a particular product. Users are not informed that their profile is being used to advertise that product. In reference to the law “Right of Publicity” (Winn & Wright, 2002, para. 1), McGeveran states, "I don’t see how broad general consent to share one’s information translates into the specific written consent necessary for advertisers to use one’s name and often picture under this law." (McGeveran, 2007, para. 7) As more law practitioners publish work on this topic, it is highly likely that consensus will dictate that social advertisements violate provisions of “Right of Publicity.” (Winn & Wright, 2002, para. 1) Facebook's use of social advertisements is just one example of how social networks are contributing to the infringement of the public's “Right of Publicity” (Winn & Wright, 2002, para. 1) There have been reports that MySpace sells its member's profile information to the highest bidder. Furthermore, additional social advertisement programs are continuing to emerge on various online social networks. Even MySpace has implemented a new advertising program that is remarkably similar to Facebook's Beacon program. If cases involving social advertisements continue to be ignored by the courts, then it is likely that social advertisements will flourish and will rapidly spread to other websites.

There are several obstacles that make it difficult to prosecute online social networking websites on the grounds of “Right of Publicity.” (Winn & Wright, 2002, para. 1) For years cases that involved "Appropriation of Name or Likeness," set the precedent that the law pertained only to public figures. Famous cases like *ETW CORP. v. JIREH PUBLISHING, 332 F.3d 915 (6th Cir. 2003) No. 00--3584* provided little justification for private individuals to file claims under the “Right of Publicity.” (Winn & Wright, 2002, para. 1) There was also a lack of precedent for resolving cases related to social

networking websites in violation of the “Right of Publicity” (Winn & Wright, 2002, para. 1) law. In 2008, precedent was finally provided in the case *Doe v. Friendfinder Network Inc*. In *Doe v. Friendfinder Network Inc*, "the plaintiff, identified as Jane Doe, sued the adult social networking service Friendfinder after learning that someone had posted a user profile describing her and attributing to her an interest in various illicit activities. In response to Doe's request, Friendfinder removed the false profile, but posted the notice "sorry, this member has removed his/her profile," which Doe complained created the false impression that she had been a member of the community and had actually posted the profile." (Winn & Wright, 2002, para. 6) The district court provided a judgment in favor of the plaintiff and "found that an online service provider (i.e., Facebook, MySpace, and Google) was not shielded by the safe harbor of Section 230 of the Communications Decency Act (CDA) from a claim of infringing a right of publicity." (Winn & Wright, 2002, para. 6) This case is significant because it provided the precedent for a private individual to sue an online social networking service on the grounds of “Right of Publicity.” (Winn & Wright, 2002, para. 6)

Based on current tort law and legal precedent, the most successful means of prevailing against a social networking website in court, is to base a claim as a violation of the “Right of Publicity” (Winn & Wright, 2002, para. 6). The case *Doe v. Friendfinder Network Inc.* provides the most effective precedent for circumventing the protective provisions of the Communications Decency Act of 1996. Programs like Facebook's Beacon are becoming more and more common. As online social networks scramble to exploit the greatest possible profit from their members, they are starting to infringe upon their members’ right to privacy and beginning to invade their personal and intellectual property (i.e.,

name, identity, depiction). However, tort laws such as “Right of Publicity” (Winn & Wright, 2002, para. 1), that are empowered by precedent setting cases like *Doe v. Friendfinder Network Inc.*, provide the public with some recourse or protection from some of the invasions of privacy that online social networking can facilitate.

DISCUSSION

By analyzing tort law, this study has clearly shown two ways that online social networking can facilitate negative societal affects. First, it has been shown that online social networking provides a medium through which members can inadvertently break laws like "Public disclosure of Private Facts" (Scott, 2006, para. 1). Second, it has been shown that online social networking can create invasive advertising that violates privacy and intellectual property laws like the “Right of Publicity” (Winn & Wright, 2002, para. 1).

Examining the law provides a very objective means of analyzing the negative effects of online social networks. Laws are primarily used as a way to run society efficiently and effectively while providing protection for citizens and their government. In short, laws are commonly used for the betterment of society. Therefore, if something is against the law, then it is likely that this action has some sort of negative impact on society. Examining the laws of “Right of Publicity” (Winn & Wright, 2002, para. 1), and “Public Disclosure of Private Facts” (Scott, 2006, para. 1), provides evidence that online social networks contribute to illicit activity. Any contribution to illicit activity negatively impacts society. Therefore social networking has some significant negative effects on society.

FURTHER RESEARCH

This study was inspired by a desire to explore how emerging technologies are governed by ageing laws. Can current law protect the public from revolutionary and evolutionary technological innovations? This is a perpetual question for which mankind will continue to seek the answer. More research and debate is needed on how traditional law will hold up in the digital age. An area of related interest is streaming digital media. Websites like Pandora.com and Hulu.com are revolutionizing the way people transmit data and multimedia. Another emerging technology is mobile social networking. Mobile networking is basically a cell phone version of an online social network. As these new technologies emerge legal thinkers need to assess whether or not current law provides ample protection.

This paper could study only a fraction of the right to privacy. Further research is needed in regards to case law. While numerous cases were presented the study did not find any examples in which ones use of an online social network was defined an action that can contribute to ones status of public figure. Such a case would be of great benefit to this work.

A better understanding of current politics behind the public figure doctrine would also be beneficial. Who believes and advocates that the doctrine should remain unchanged? Have any politicians noted the relationship between the doctrine and online social network use?

A better understanding of the psychological effects of online social network would also provide invaluable insight. Can online social networking be addictive? Can online social

networking inhibit or promote depression? In discussing the negative effects of online social networking few questions would be more interesting.

Further research should also examine the sociological factors related to online social networks. Have the networks altered the norms of socialization? Do these networks promote or discourage social isolation? Have these networks increased social communication? The impact of online social networks would be truly enlightening.

REFERENCES

Aikins, Herbert Austin. *The Principles of Logic*. H. Holt and company, 1902. Print.

Boyd, Danah M. and Ellison, Nicole B. *Social Network Sites: Definition, History, and Scholarship* . Web. January 2008.

Breckenridge, Adam Carlyle. The Right to Privacy. U of Nebraska Press, 1970. Print.

Browne, Harry. *Does the Constitution Contain a Right to Privacy?* harrybrowne.org. Web. May 2008.

Chen, Hsinchun and Zeng, Daniel. *National security.* Emerald Publishing, 2007. Print

Cohen, Michael L. White, Andrew A. Rust, Keith. and National Research Council (U.S.). Panel to Evaluate Alternative Census Methodologies. *Measuring a changing nation: modern methods for the 2000 census Compass series.* National Academies Press, 1999. Print

Davidson, Margaret Ferrol. *A Guide for Nnewspaper Stringers*. Routledge, 1990. Print

Deibert, Ronald. Palfrey, John G. Rohozinski, Rafal.and Zittrain, Jonathan. *Access Denied: The Practice and Policy of Global Internet Filtering*. MIT Press, 2008. Print

Delta, G and Matsuura, J. *Treatise, Law-of-the-Internet, § 6.01 Copyright. Law-of-the-Internet, 3.* Computer and Internet Law Integrated Library database. Web. 27 October 2008.

Delta, G and Matsuura, J. *Treatise, Law-of-the-Internet, § 6.015 Fair Use. Law-of-the-Internet, 3.* Computer and Internet Law integrated Library database. Web. 27 October 2008.

Delta, G and Matsuura, J. *Treatise, Law-of-the-Internet, § 6.04 Digital Format Licenses. Law-of-the-Internet, 3.* Computer and Internet Law Integrated Library database. Web. 27 October, 2008.

Delta, G and Matsuura, J. *Treatise, Law-of-the-Internet, § 6.06 Vicarious Liability / Contributory Infringement. Law-of-the-Internet, 3.* Computer and Internet Law Integrated Library database. Web. 27 October 2008.

Delta, G and Matsuura, J. *Treatise, Law-of-the-Internet, § 6.07 Web Content Management. Law-of-the-Internet, 3.* Computer and Internet Law Integrated Library database. Web. 27 October 2008.

Delta, G and Matsuura, J. *Treatise, Law-of-the-Internet, § 6.18 User Generated Content. Law-of-the-Internet, 3.* Computer and Internet Law Integrated Library database. Web. 27 October 2008.

Delta, G and Matsuura, J. *Treatise, Law-of-the-Internet, § 6.19 Role of Intermediaries. Law-of-the-Internet, 3.* Computer and Internet Law Integrated Library database. Web. 27 October 2008.

Doe v. MySpace and News Corporation. US District Court, Western District of Texas. 16 May 2008.

Dyché, Jill. *The CRM handbook: a business guide to customer relationship management.* Addison Wesley, 2002. Print

Einsohn, Amy. *The copyeditor's handbook: a guide for book publishing and corporate communications, with exercises and answer keys.* University of California Press, 2000. Print

Estill v. Hearst Publishing Co. No. 10272. US Court of Appeals Seventh Circuit. 29 January 1951.

ETW Corporation v. Jireh Publishing. 03a0207p. US Court of Appeals, 6th Circuit. 20 June 2003.

Facebook. *Facebook Unveils Facebook Ads*. Facebook.com. Web. 20 November 2008.

Farkas, Meredith G. *Social software in libraries: building collaboration, communication, and Community Online.* Information Today, 2007. Print.

Garrett, Brandon. *The Right to Privacy- Individual Rights and Civic Responsibility Series.* The Rosen Publishing Group, 2001. Print.

Gertz v. Robert Welch, Inc. no. 72-617. Supreme Ct. of the US. 25 June 1974.

Griswold V. Connecticut. No. 496. Supreme Ct. of the US. 7 June 1965.

United States. Cong. House. Deleting Online Predators Act of 2006. 109th Congress, 2nd session. HR 5319. Washington: GOP, 2006.

United States. Cong. House. Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act of 2009. 111th Congress, 1st session. HR 1076. Washington: GOP, 2009.

Hall, Kermit L. The Oxford guide to United States Supreme Court decisions. Oxford University Press, 2001. Print.

Kant, Immanuel. Pluhar, Werner S. Kitcher, Patricia. *Critique of pure reason.* Hackett Publishing, 1996. Print.

Kay, Russell. *Online Social Networking These sites can facilitate connections in your industry or around the world.* computerworld.com. Web. May 2009.

Levitt, Carole A. and Rosch,Mark E. *The lawyer's guide to fact finding on the Internet. American Bar Association.* American Bar Association, 2006. Print.

Loughlin, Martin. *Sword and scales: an examination of the relationship between law and politics.* Hart, 2000. Print.

Masanès, Julien. *Web archiving.* Springer, 2006. Print

McGeveran, W. *Info / Law.* blogs.law.harvard.edu. Web. November 2008.

MySpace Surpasses Yahoo Mail, Google in Popularity. marketingvox.com. Web. December 2008.

O'Neill, Nick. *Facebook Takes the Lead.* allfacebook.com. Web. March 2009.

Panos; Patrick. *The Internet Archive: An End to the Digital Dark Age*. Journal of Social Work Education, Vol. 39, (2003). questia.com. Web. December 2009.

Patańjali. *The Yoga Sutras of Patańjali*. Translated by James Haughton Woods. Courier Dover Publications, 2003. Print.

Phillips, Margaret. *PANDORA, Australia's Web Archive, and the Digital Archiving System that Supports it.The role of national libraries in Web harvesting.* DigiCULT.info, Issue 6, (2003) Digital Archiving, National Library of Australia. April 2009.

Phillips, Patti. *Converting Data to Monetary Value.* ROI Institute. Web. March 2009.

Piccard, Paul L. Marcus. *Securing IM and P2P applications for the enterprise.* Syngress, 2006. Print.

Rheingold, Howard. *Smart mobs: the next social revolution, Part 3*

http://books.google.com/books?id=zpArKHohtCMC&pg=PA14&dq=by+Jarkko+Oikarinen+in+1988.#v=onepage&q=by%20Jarkko%20Oikarinen%20in%201988.&f=false

Richard, Mark. Prepared statement of the United States of America. Presented at EU Forum on Cybercrime. Brussels, 27 November 2001.

Scheppele, Kim Lane. *Legal secret: equality efficiency in the common law*. University of Chicago Press, 1988. Print.

Scott, Michael. (2006). *Treatise, Scott-Information-Technology, §16.06C Public Disclosure of Private Facts. Scott-Information-Technology, 3.* Computer and Internet Law Integrated Library database. Web. 27 October 2008.

Smith, Robert Ellis. *The Law of Privacy Explained.* Web. May 2009

Sundén, J. Material. *Material Virtualities: Approaching Online Textual Embodiment.* New York: Peter Lang, 2003. Print.

The economist, *Volume 358*. Economist Newspaper Ltd, 2001. Print.

The journal of philosophy, psychology and scientific methods, *Volume 5*. JSTOR. Science Press, 1908. Print.

The journal of philosophy, psychology and scientific methods, *Volume 12*. JSTOR. Science Press, 1915. Print.

Time, Inc. v. Hill. No. 22. Supreme Ct. of the US. January 9, 1967

Weber, Larry. *Marketing to the social web: how digital customer communities build your business*. John Wiley and Sons, 2007. Print

Wilson, Brian C. Light, Timothy. *Religion as a human capacity: a festschrift in honor of E. Thomas Lawson.* Brill, 2004. Print.

Winn, Jane & Wright, Benjamin. (2002). *Treatise, Law-of-Electronic-Commerce, § 2.02 Online. Service Providers. Law-of-Electronic-Commerce, 4.* Computer and Internet Law Integrated Library database. Retrieved October 2008.

Winn, Jane & Wright, Benjamin. (2002). *Treatise, Law-of-Electronic-Commerce, § 14.03 Privacy Rights. Law-of-Electronic-Commerce, 4.* Computer and Internet Law Integrated Library database. Retrieved October 2008.

Winn, Jane & Wright, Benjamin. (2002). *Treatise, Law-of-Electronic-Commerce, § 14.09 Right of Publicity. Law-of-Electronic-Commerce, 4.* Computer and Internet Law Integrated Library database. Retrieved October 2008.

Wollstonecraft, Mary. *A vindication of the rights of woman.* Walter Scott, 1891. Print.