The Historical Society *of the* New York Courts

Gaitrie Singh

2013 David A. Garfinkel Essay Contest
CUNY Community College Prize

Personal Privacy vs. Digital Lives

Faculty: Professor Christine Mooney
Queensborough Community College

Personal Privacy vs. Digital Lives

Today the internet plays a huge role in our everyday lives. We use it constantly for connecting with friends on social networks, online shopping, and applying for jobs. You may assume paying for your own internet service means everything you do on it is private and protected. Instead, the internet remains largely unregulated and the laws regarding privacy are still being developed.

Personal privacy is a reasonably new legal concept which is frequently evolving. Corporations are silently on the move to learn more about our habits and preferences to help boost their revenues.[1] The majority of web users are hidden from the fact that websites already record our every click, and email services without our consent. The companies who collect information on everything we do online are known as data aggregators.[2] Users are being discriminated on websites due to what they searched in the past. For example, author Lori Andrews stated in her interview with ABA Journal web producer, Lee Rawles:

> You can do a Google search for a medical condition and go on a life insurance website where you would be denied life insurance or be given a lower amount based on the assumption that you have that disease, even if you are looking it up for someone else. People are being judged based on what an aggregated group of people would do rather than an individual.[3]

Everything we do on the internet is tracked, saved, and can be used against us in the future.

Have you ever wondered how the internet can use our browsing history to release our information to other companies and people? When signing up for internet service, your Internet Service Provider gives you an Internet Protocol (IP) address, which is a possible weak link when it comes to protecting your privacy.[4] Privacy Rights Clearinghouse briefly explains parts of our browsers and how they can publish our searches:

> Your browser likely provides your IP address and information about which sites you have visited to Web site operators. As you move from site to site online, numerous companies utilize sophisticated methods to track and identify you . . . Search engines have and use the ability to track each one of your searches. They can record your IP address, the search term you used, the time of your search, and other information . . . The Web server may use cookies to keep track of the different pages within the site that the user accesses. However, there are some cookies, called third-party cookies that communicate data about you to an advertising clearinghouse which in turn shares that data with other online marketers. These third-party cookies include “tracking cookies” which use your online history to deliver other ads.[5]

There are numerous ways the internet can expose our searches to various businesses through our digital footprints. Our searches reveal personal information about us, such as our likes or dislikes, favorite clothing stores, and future vacation areas.

The main risk in the digital world is what is being kept private and parties against which privacy is being evoked.[6] Two notions of privacy mentioned in the National Academies podcast are confidentiality, secrecy of some specific information; and anonymity, unattributed publication of an article and so forth.[7] An example mentioned was "an employer may be concerned that an article contains trade secrets or a company's proprietary information and want to identify the source of that info," and privacy rights are often invoked to prevent the disclosure of such information.[8] Even though privacy is the main concern throughout the web, our personal information is also at risk on the computer systems. In a civil issue, *Ingenix, Inc. v. Lagalante,* 2002:

> Defendant left his employment with the Plaintiff to work for Plaintiff's competitor as a vice president of sales. The Plaintiff (Defendant's former employer) filed suit against Defendant alleging fraudulent, abusive, and knowing misappropriation of computer files and proprietary information causing damage in excess of $5,000 in violation of the Computer Fraud and Abuse Act. While the CFAA is a criminal statute, the court affirmed the rule that a violation of the statute can provide the basis for civil liability. Plaintiff's allegations were based upon evidence that the Defendant had misused his company laptop and took steps to appropriate data relating to customers "in the sales funnel" for his new employer. A computer forensic examination of email messages sent by Defendant and the pattern of Defendant's use and downloading of files from his laptop revealed that he had, in fact, downloaded and deleted confidential and proprietary customer information for use by Plaintiff's competitor.[9]

Once our personal information is programmed in any type of computer system, we are highly at risk for basically any sort of catastrophe happening with our data.

Throughout history, privacy has always been a major conflict concerning an individual's personal life. The idea of a right to privacy in your personal life was not even conceived until the 1890s, when newspapers became more sensational with stories of gossip and sexual scandal.[10] Ever since, it has been a long, hard battle from the adoption of the federal statute to protect the privacy of conversation in 1968 to the current issue of privacy in our digital lives today. In fact, our First and Fourth Amendment rights have been altered due to various trials.

Our daily lives consist of social networking, indulging in various media sources, constantly learning or searching new information on the web. The creation of these websites was meant for us to freely explore and

connect with friends and family and help make our lives a little easier and more enjoyable. In fact, scholar and writer Stephen E. Henderson informs us that "the first amendment's freedom of speech protects privacy in the form of anonymous speech, and the Supreme Court has interpreted the Bill of Rights to include substantive due process protection for private decisions."[11] However, our freedom, privacy, and other values held for citizens in the U.S. changed through recent terrorist attacks in our country. The tragic loss of thousands of innocent human lives from the September 11th terrorist attacks on the World Trade Center resulted in increased surveillance of all communications. Meaning the internet, wireless, wire-lines, and satellites are strictly monitored, all website activity monitoring and data collection are tracked, access to personal and business records of all kinds, and much more limitations.[12] Even though it places such strict warnings and sheds us of our online privacy, it could potentially reveal plans of suspects proactively to provide advance warning.[13] The USA Patriot Act is an Act of the U.S. Congress that was signed into law by President George W. Bush on October 26, 2001:

> The USA PATRIOT Act, passed by congress after the terrorist attacks of September 11, 2001, and amended in 2006, makes it easier for the government to access records about online activity. In an effort to increase the speed in which records are acquired, the Act eliminates much of the oversight provided by other branches of the government. And it expands the types of records that can be sought without a court order.[14]

This Act may protect us from future attacks, but we no longer have privacy rights. Our every move on the web is being tracked, and what we look at can come back to haunt us.

These constant changes in society that are linked to our privacy disrupts more than our amendments. Court cases are being reshaped about social networks, and the majority of the time it confuses them.[15] Due to the fact that a social network, like Facebook, can be very misleading in a case if it revolves around a minor who just enjoys making silly jokes with his/her friends, but can be seen differently in a court room. The National Research Council cites three major drivers of vast changes affecting notions, perceptions and expectations of privacy:

1. Technological - major influence on today's social and legal regime governing privacy. The frequent increasing storage space stores too much information that can include any sort of information for a very long time.
2. Societal Shifts - evolutional changes in institutions of society making personal information available to institutions has become essential for individual participation in everyday life.
3. Discontinuities in circumstance – events and concerns that utterly transform the national debate on privacy.[16]

A number of state constitutions explicitly protect privacy, and the law has not been stagnant but instead in every category has adapted to the changing circumstances of over two hundred years.[17]

How much privacy do we really have today? We may use our personal computers to surf the internet for our personal needs, but how many others can see what we are doing? In a lot of cases, you will apply for a job and employers will start doing online searches to figure out what type of person you are. Employers can search and analyze your Facebook page and would not want you because of certain things you liked on Facebook, because in some cases they do not have to right to bring a health issue during an interview.[18]

In most cases, rights to privacy can be disregarded depending on certain cases. The Privacy Rights Clearinghouse states that:

> In U.S. v Warshak (decided December 14, 2010); the Sixth Circuit Court of Appeals ruled that although an ISP has access to private e-mail, the government must obtain a search warrant before seizing such e-mail. The issue that the court dealt with in this case was the expectation of privacy that is afforded to e-mail hosted on a remote server. The court stated: Given the fundamental similarities between email and traditional forms of communication [like postal mail and telephone calls], it would defy common sense to afford emails lesser Fourth Amendment protection.... It follows that email requires strong protection under the Fourth Amendment; otherwise the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve...[19]

This case strongly supports the Fourth Amendment, which provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[20] However, rights to privacy are lessened in cases such as private email. For instance, judges are allowing social networking in sexual abuse cases, such as the 13-year-old sex life online. As time passes, all the activities we do online, including downloading music, are continuously being tracked. Corporate counsel Lisa Shuchman informs us on the Entertainment industry's latest effort to combat piracy:

> The Copyright Alert System (CAS), also known as the "six strikes policy," is a program created by the Motion Picture Association of America (MPAA), the Recording Industry of America (RIAA), and the five largest Internet Service providers – AT&T, Cablevision, Comcast, Time Warner, and Verizon. The program, according to its creators, was established to "educate" web users who download copyrighted music, films, and other materials.[21]

Again, this personal activity we do in our homes will be tracked through our ISP numbers.

Freedom of expression is a right we are slowly losing. The real question is how much more will it change and affect our future generations. David Shenk mentions in his article:

> Websites already silently record our every click, and e-mail services such as Google's Gmail expose our messages to machine analysis. In coming years, many other consumer objects will root out and transmit our private data. The retail industry is well on its way to including tin radiofrequency identification tags with every consumer product from underwear to milk cartons to brake pads (spy chips). . . The hallmarks of the new digital age are machines that are increasingly smart, small, cheap and communicative. We are, without question, headed into a world in which-mostly by our choice-the minute details of our bodies, lives and homes will be routinely tracked and shared, with the potential for more convenience and safety but also abuse. On the one hand, most of us will trade our anonymity and privacy for increased national security and cleaner, healthier and easier lives. On the other hand, we will be more vulnerable not only to malicious hackers and identify thieves but also to sophisticated marketers.[22]

Possible violation of constitutional rights will occur if this digital age keeps going down the same path without establishing any type of law for an individual's protection. It is very unfair that we have to sacrifice our personal privacy because of others who cause danger and harm to us. Samuel Warren and Louis Brandeis, two young lawyers who were prominent in Boston society, published their novel idea in a *Harvard Law Review* essay "Personal privacy is the *right to be left alone."*[23] Every week a new scandal seems to outburst with the social network highly involved in the cases. So now the Obama Administration is saying enough is enough, and has proposed a Consumer Privacy Bill of Rights that it hopes will lead to new regulations on tech companies.[24] This would help companies to follow reasonable limits on how much information they gather about consumers and share.

Balancing our digital lives and our personal privacy can be a difficult task. We create a profile on social networks to express ourselves and communicate with friends, who we are very comfortable with and can say anything too. What individuals have to focus primarily on is how they communicate to others and question themselves as to whether what they are posting is offensive or disrespectful to others. Henderson cited that the Court has articulated this general principle:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[25]

Based on all the heinous events the United States has faced, especially after 9/11, the term personal privacy now consists of limitations and our "freedom of speech" can be used against us any time.

In summary, personal privacy can be easily traced with today's ever-changing technology. Computers and the internet provide the ability to rummage through the closets of our lives in ways that have never before been possible. Privacy may be an option when we set it on our web accounts, but the search engines can backfire unless we are careful and alert.

Endnotes

1 David Shenk, "Surveillance Society: Openness is the best defense against intrusions into our private realms," EMBO *reports*, 7 (2006): S31. National Center for Biotechnology Information. 6 April 2013 <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1490309/>.
2 Lee Rawles, "I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy," http://www.abajournal.com/books/article/podcast_episode_004/
3 *Id.*
4 "Fact Sheet 18: Online Privacy: Using the Internet Safely." December 2012. Privacy Rights Clearinghouse. 22 February 2013 <https://www.privacyrights.org/fs/fs18-cyb.htm>.
5 *Id.*
6 Anne Merchant, "Sounds of Science: Engaging Privacy and Information Technology in a Digital Age," http://www.nap.edu/audioplayer.php?record_id=11896&n=0.
7 *Id.*
8 *Id.*
9 *Case Law: Civil Issues.* Georgia Bureau of Investigation. 26 February 2009. <http://familyinternet.info/Cases_7.htm>.
10 Clarence Jones. "Privacy: Get out of here . . . and Leave Me Alone." 2005. Winning with the News Media. 22 February 2013 < http://winning-newsmedia.com/privacy.htm>.
11 Stephen E. Henderson. "Expectations of Privacy in Social Media." (March 8 2012). Mississippi College Law Review, Vol. 31, 2012. <http://ssrn.com/abstract=2018425>.
12 Bharath Krishnamurthy. "Privacy vs. Security in the Aftermath of the September 11 Terrorist Attacks." Markkula Center for Applied Ethics, Santa Clara University. 1 November 2001. <http://www.scu.edu/ethics/publications/briefings/privacy.html>.
13 *Id.*
14 Fact Sheet 18: Online Privacy: Using the Internet Safely, https://www.privacyrights.org/fs/fs18-cyb.htm
15 Rawles, "I know who you are and I saw What You Did: Social Networks and the Death of Privacy."
16 Anne Merchant, "Sounds of Science: Engaging Privacy and Information Technology in a Digital Age."
17 Henderson, 231.
18 Rawles, "I know who you are and I saw What You Did: Social Networks and the Death of Privacy."
19 Fact Sheet 18: Online Privacy: Using the Internet Safely, https://www.privacyrights.org/fs/fs18-cyb.htm
20 U.S. Const. amend. IV.
21 Lisa Shuchman, "Controversial Copyright Alert System to Combat Online Piracy," 26 February 2013, ALM Media Properties, 7 April 2013 http://www.law.com/corporatecounsel/PubArticleCC.jsp?id=1202589552962&Controversial_Copyright_Alert_System_to_Combat_Online_Piracy&slreturn=20130307060402
22 Shenk, S31.

23 Clarence Jones. “Privacy: Get out of here . . . and Leave Me Alone.”
24 Dan Lyons, “Obama Pushes for New Internet-Privacy Law to Protect Consumers,” *The Daily Beast.* February 23, 2012. < http://www.thedailybeast.com/articles/2012/02/23/obama-pushes-for-new-internet-privacy-law-to-protect-consumers.html>.
25 Henderson**,** *cited* Katz v. United States, 389 U.S. 347,351 (1967).

Works Cited

Andrews, Lori. Interview by Lee Rawles. “I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy.” *ABA Journal Law News Now.* American Bar Association. 29 May 2012. Web. 2 April 2013.

“Case Law: Civil Issues.”*ICAC Task Force.* Georgia Bureau of Investigation. 26 February 2009. Web. 5 April 2013.

“Fact Sheet 18: Online Privacy: Using the Internet Safely.” *Privacy Rights Clearinghouse.* July 1995 revised March 2013. Web. 2 April 2013.

Henderson, Stephen E. “Expectations of Privacy in Social Media.” Mississippi College Law Review, Vol. 31. 8 March 2012. Web. 3 April 2013.

Jones, Clarence. “Privacy: Get out of here . . . And Leave Me Alone.” *Winning with the News Media.* 2005. Web. 22 February 2013.

Krishnamurthy, Bharath. “Privacy vs. Security in the Aftermath of the September 11 Terrorist Attacks.” *Santa Clara University.* Markkula Center for Applied. 1 November 2001. Web. 22 February 2013.

Lin, Herbert S.; Merchant, Anne; Millet, Lynette I.; Waldo, James. “Engaging Privacy and Information Technology in a Digital Age.” *The National Academies Press.* National Academy of Sciences. 2007. Web. 1 April 2013.

Lyons, Dan. “Obama Pushes for New Internet-Privacy Law to Protect Consumers.” *The Daily Beast – U.S. News.* The Newsweek/Daily Beast Company LLC. 23 February 2012. Web. 6 April 2013.

Shenk, David. “Surveillance Society: Openness is the best defense against intrusions into our private realms.” *Embo Reports* (2006). n.p. Web 2 April 2013.

Shuchman, Lisa. “Controversial Copyright Alert System to Combat Online Piracy.” *Connecticut Law Tribune.* ALM website. 26 February 2013. Web. 2 April 2013.