

I KNOW WHO YOU ARE AND I SAW WHAT YOU DID
[SOCIAL NETWORKS AND THE DEATH OF PRIVACY]

Justin McHugh¹

Citation: LORI ANDREWS, *I KNOW WHO YOU ARE AND I SAW WHAT YOU DID* (Free Press ed., 2011).

Relevant Legal and Academic Areas: Constitutional Law, Intellectual Property Law, Tort Law, Internet Law, Criminal Law, Privacy, Social Media, Facebook, Twitter, Google, YouTube, and Myspace.

Summary: *I Know Who You Are And I Saw What You Did [Social Networks and the Death of Privacy]* is a book pertaining to the Internet and specifically social media. The book describes the downward spiral that social media is having on society and the desperate need for change. Sadly, the law has not yet caught up with the ever changing technology and changings in social media. Every day the Internet and specifically social media is encroaching on our fundamental rights of expression and speech. Social media which was once a tool to expand freedom of expression has now turned into a tool of restriction. Internet and more specifically social media users need to wake up and take action before the Internet completely restricts their fundamental rights of expression and speech.

About the Author: Lori Andrews is a law professor that has focused her career on Law and Technology. She has been published numerous times and has often been a guest on *Oprah*, *60 Minutes*, and *Nightline*.² Lori Andrews is a very influential lawyer who has used her expertise in Law and technology to advice the United States government on many issues pertaining to the ethical and legal issues surrounding the ever advancing technology that we use every day.

¹ Syracuse University College of Law, Juris Doctor expected 2015.

² LORI ANDREWS, *I KNOW WHO YOU ARE AND I SAW WHAT YOU DID* (Free Press ed., 2011).

I. INTRODUCTION

In this section the background of how social media, specifically Facebook, and the Internet track and use our information to market us products and develop an unrealistic model of our real selves.

A. Facebook Nation

Since the creation of Facebook, people have been flocking to social media to have their voices heard. Facebook now has over 750 million members making it the “third largest nation in the world.”³ With so many followers, Facebook has essentially become its own nation with its own followers, financial system, legal system, and relationships with fellow real world nations.⁴ Just like with any nation, there are issues of privacy and governmental intrusion into people’s lives. Generally, Facebook and the Internet have never given great reverence to users’ privacy. Instead, Facebook and sites like Spokeo continue to collect data on people and sell it to the highest bidder.⁵ Spokeo and Facebook are a part of a “multibillion-dollar industry of data aggregators.”⁶ These companies take Internet users data, bundle it up into neat little packages, and sell it to all sorts of interested third parties.⁷ Advertising agencies, businesses, and

³ ANDREWS, *supra* note 2, at 1.

⁴ *Id.* at 2.

⁵ *Id.* at 11.

⁶ *Id.*

⁷ *Id.*

government agencies can all benefit from the research and use of this data.⁸ Advertising agencies can develop more narrowly tailored marketing strategies to get individuals to buy things that they do not really need.⁹ Businesses can perform intrusive background checks on potential employees.¹⁰ Lastly, the government or big brother can keep a better eye on us with promises of better security and protection.¹¹ The true repercussions of the continued sale of our search histories and Internet use are the loss of our privacy. Sadly, one judge even went as far to say that once you start using Internet services, “the right to privacy is lost, upon your affirmative keystroke.”¹²

Social networks have the ability to bring a vast array of potential benefits such as being able to keep in touch with friends and family, stay up to date with the news, and interact with and be heard by the government and politicians, but at what cost?¹³ People have been attracted to social media sites like Facebook so that they can express their ever evolving social self.¹⁴ What most users fail to realize is that their expressions and opinions are being used by businesses to turn a profit. People started using Facebook and the Internet as a way to freely express their beliefs and values while interacting with other like-minded individuals.¹⁵ “But unless people’s rights [to privacy] are protected, social networks [and the Internet] will [only] serve to narrow

⁸ ANDREWS, *supra* note 2, at 11.

⁹ *See id.*

¹⁰ ANDREWS, *supra* note 2, at 11.

¹¹ *Id.*

¹² *Id.*

¹³ *Id.* at 12-13.

¹⁴ *Id.* at 13.

¹⁵ ANDREWS, *supra* note 2, at 13.

people's behavior and limit their opportunities, rather than expand them."¹⁶ The continued intrusion and eventual elimination of Internet user's privacy rights will only bring negative repercussions. There have already been specific examples seen where employees or potential employees have been fired or denied a job opportunity because of their private actions online.¹⁷ If Facebook and Internet users do not smarten up and take charge of their privacy rights, they may soon find that nothing in their lives is private anymore.

B. George Orwell...Meet Mark Zuckerberg

From the moment we log onto the Internet our every move is being tracked, detailed, and stored by "data aggregators" who then use this supposedly private information to tailor marketing campaigns and ads directly to our likes and dislikes.¹⁸ The reason for this ever increasing desire for our private information is known as "behavioral advertising".¹⁹ The Federal Trade Commission has categorized "behavioral advertising [as] the tracking of consumers' online activities in order to deliver tailored advertising."²⁰ Through the use of behavioral advertising, businesses are better able to target individuals and market specific products to them that they are more likely to buy according to their Internet footprint.²¹ This type of narrowly targeted advertising has led to a tremendous increase in profits for the businesses that practice

¹⁶ *Id.*

¹⁷ *See id.*

¹⁸ ANDREWS, *supra* note 2, at 18.

¹⁹ *Id.*

²⁰ *Id.*

²¹ *See id.*

it.²² Facebook is one of the most well-known businesses that mine our personal information and sell it to third party companies who use the information in their behavioral advertising strategies.²³ One of the negative effects of companies like Facebook collecting and selling our personal information that is only now starting to be fully understood has become known as “weblining.”²⁴ “Weblining” was developed to describe the negative effects that our digital trails online can have on our potential economic and social opportunities.²⁵ There can be serious side effects based solely on the interactions people have online. Depending on what people do online can severely affect the opportunities that will be offered to them.²⁶ These missed opportunities can come in the form of missed discounts, higher interest rates, and decreased credit lines to name a few.²⁷

One of the major downside to weblining is that it can literally narrow the type of information that we see and access online.²⁸ Narrowing the information we see and have access to online can have a direct effect on the way we perceive the world around us. Eli Pariser summed it up best when he stated that “Ultimately, democracy works only if we citizens are capable of thinking beyond our narrow self-interest. But to do so, we need a shared view of the world we cohabit.”²⁹ Having our interests dictate what we see online deprives us of seeing ideas

²² ANDREWS, *supra* note 2, at 18.

²³ *Id.* at 19.

²⁴ *Id.* at 19-20.

²⁵ *Id.* at 20.

²⁶ *Id.* at 20-21.

²⁷ ANDREWS, *supra* note 2, at 20-21.

²⁸ *Id.* at 21.

²⁹ *Id.*

from a different perspective. Ultimately, this online personalization can cause us to become more narcissistic and narrow minded individuals.³⁰

Online personalization, curtailing, and narrowing the type of information we see online are based on the websites we visit and the way third parties track our movements online.³¹ Companies like Comcast use tracking tools to follow us online and store data on our habits and preferences.³² This surveillance information is used to create an image of a person that will better help third parties market and sell products to them.³³ Data mining is big business and helps companies to develop an image of your online self, known as your “second self.”³⁴ The problem is that this second self is usually distorted and not accurate of the user it is trying to portray.³⁵ This distortion comes from the fact that the same user does not always use the same computer or may be searching online for someone other than themselves.³⁶ Collectors of our online data do not account for all the potential variables that may affect how we come across online. One consequence of this is that behavioral advertisers will use distorted online tracking information to predetermine what we see online.³⁷ As previously mentioned, this can lead to less freedom online and a more narrow view of what we see and are able to interact with online.³⁸

³⁰ *See id.*

³¹ ANDREWS, *supra* note 2, at 21-23.

³² *Id.* at 22.

³³ *Id.* at 22-25.

³⁴ *Id.* at 28.

³⁵ *Id.* at 18-29.

³⁶ ANDREWS, *supra* note 2, at 28-29.

³⁷ *Id.*

³⁸ *Id.* at 29.

What is even more horrifying is that “[o]ur digital doppelgangers are directing our futures and the future of society” through distorted images that narrow our opportunities and proliferate stereotypes.³⁹

C. *Second Self*

The image that we create of ourselves through our use of social media is often distorted due to the lack of regulations on the collection of our personal data and the intrusions into our privacy. The Federal Trade Commission is only now starting to create new ways to regulate the way our information is collected and used to market us products.⁴⁰ There are numerous federal laws that can be applied to the collection of online data in order to protect the privacy of individuals. The Computer Fraud and Abuse Act, the Stored Communications Act, and the Wiretap Act have all been used in the past to protect individual’s private information.⁴¹ The problem is that many courts have inadvertently created loopholes that privilege data aggregators over the individual’s data that they are collecting.⁴² In the landmark case *In re DoubleClick*, a New York federal judge found that the “data aggregator’s intent was not to commit a tort or a crime, but rather to make a lot of money so its activities were permissible.”⁴³

Despite the loopholes developed from some unsavory federal court decisions, there is still hope for bringing data aggregators to justice for stealing personal information. The Federal

³⁹ *Id.*

⁴⁰ *Id.* at 47.

⁴¹ ANDREWS, *supra* note 2, at 43.

⁴² *Id.*

⁴³ ANDREWS, *supra* note 2, at 44.

Trade Commission has been the leading advocate for protecting consumer's rights from social networks, advertisement agencies, and data aggregators.⁴⁴ The FTC was granted the power to protect consumers against "unfair or deceptive acts or practices."⁴⁵ Through the Federal Trade Commission, individuals can file complaints against businesses for their deceptive practices. Beginning in the early 2000s, many individuals started to file complaints against data aggregators for deceptively acquiring their personal information from the Internet.⁴⁶ The Federal Trade Commission has gone after large companies such as Google, Facebook, and many other data aggregators and has forced them to implement some privacy changes.⁴⁷

What most people fail to realize is that most companies have free rein to track and collect our personal information. Before we can develop a way to protect our privacy and second selves online, people need to become aware of how much of their personal information is actually being stolen.⁴⁸ Knowing how significantly and readily individuals' rights are being trampled on while using the Internet may be the catalyst needed for change.⁴⁹

II. ANALYSIS

This section describes how our fundamental rights are being encroached on and an analysis of what freedom of speech and expression actually means.

⁴⁴ *Id.* at 46.

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ ANDREWS, *supra* note 2, at 48.

⁴⁹ *See id.* at 47-48.

A. Technology and Fundamental Rights

Technology is continually being used to intrude into our own personal lives.⁵⁰ These intrusions are happening without our consent or our knowledge.⁵¹ The key to protecting our fundamental rights of privacy must come from knowledge and people spreading the word of exactly how our rights are being trampled on.⁵² As more and more people realize how our fundamental rights are being encroached on, there will be a greater outcry for protection.⁵³ Eventually, the law will catch up with how technology is stealing our freedom away and selling it to the highest bidder.⁵⁴ Until that day, we must be wary of our actions online and the possible repercussions they will have on our future selves. Finding a balance between wanting to stay connected with our friends and family and our ever expanding social network versus the loss of our fundamental rights is a good place to start.⁵⁵

B. The Right to Connect

Groups are using social media such as Twitter and Facebook to coordinate and plan protests.⁵⁶ Specifically, social media was used to help coordinate the protests in Egypt.⁵⁷

⁵⁰ See ANDREWS, *supra* note 2, at 49.

⁵¹ *Id.*

⁵² *Id.* at 51.

⁵³ *Id.*

⁵⁴ *Id.* at 51-53.

⁵⁵ ANDREWS, *supra* note 2, at 57-59.

⁵⁶ *Id.* at 61.

Essentially, young adults were able to organize protests and rallies all through the use of Facebook pages and Twitter accounts.⁵⁸ The potential for using social media as a medium to promote democracy and freedom became quite apparent when protests began taking place throughout Egypt.⁵⁹ It was not long before former President Hosni Mubarak saw this potential threat to his dictatorship and had the Internet shut down all throughout Egypt.⁶⁰ But by now it was too late as protestors continued to take to the streets and alleyways to proclaim their abhorrence of former President Hosni Mubarak's authoritarian practices.⁶¹ It is ironic how social media sites are helping to promote democracy at the same time as they are taking away our freedoms.

C. Freedom of Speech

The United States Constitution generally protects freedoms of speech and expression.⁶² However, when it comes to what is posted on social media sites, it would seem that for some reason these protections do not apply.⁶³ Students and teachers alike have been reprimanded for pictures or comments they have posted on social media websites.⁶⁴ In some of the more bizarre cases, students have been expelled and teachers have been fired for what seems to be very minor

⁵⁷ ANDREWS, *supra* note 2, at 61.

⁵⁸ *Id.* at 61-62.

⁵⁹ *Id.* at 61-63.

⁶⁰ *Id.* at 61-62.

⁶¹ *Id.* at 62.

⁶² ANDREWS, *supra* note 2, at 76.

⁶³ *Id.*

⁶⁴ *Id.*

offenses.⁶⁵ One student was expelled for posting comments about the poor conditions of his school on his Facebook account.⁶⁶ In another strange example, a teacher was expelled when a picture of her with a glass of wine was posted on Facebook from years ago.⁶⁷ In a Country that celebrates freedom of expression and speech, it would seem that these fundamental rights are somehow lost when using the Internet.⁶⁸ The entire concept of democracy is based on the freedom to express oneself and ideas while not encroaching on another's freedoms.⁶⁹ If freedoms of speech and expression are taken away what will be left of democracy? The author argues that people should be free and enabled to express themselves unless that speech is meant to cause imminent societal harm.⁷⁰ Expressing one's likes and dislikes is a basic staple of democracy that can help enable societal change where needed.⁷¹ Social media was meant to enable users to express their ideas and beliefs. Instead of expanding freedoms of speech and expression, it would seem that individuals are losing these fundamental rights.⁷²

D. Lethal Advocacy

Numerous individuals are turning to social media to express their most intimate secrets and feelings. Nadia Kajouji, an 18-year-old student at Carleton University in Ontario, Canada

⁶⁵ *Id.* at 76-77.

⁶⁶ *Id.* at 76.

⁶⁷ ANDREWS, *supra* note 2, at 76-77.

⁶⁸ *Id.* at 77.

⁶⁹ *Id.* at 90.

⁷⁰ *Id.*

⁷¹ *Id.*

⁷² ANDREWS, *supra* note 2, at 89-90.

used social media to describe her downward spiral into depression.⁷³ Through her use of social media sites, Nadia was able to find someone whom she thought really understood the type of depression she was going through.⁷⁴ On a social network, Nadia met a young American nurse, Cami, who claimed to be suffering from depression as well.⁷⁵ Nadia believed that she had finally found someone who understood what she was going through, in reality this could not have been further from the truth.⁷⁶ The truth was that Cami was not the name of a young American nurse suffering from depression.⁷⁷ Cami was a “46-year-old man, William Francis Melchert-Dinkel, who got his sick kicks out of attempting to convince young women to slash their wrists or hang themselves in front of a webcam so he could watch.”⁷⁸ Cami, who was actually William Francis Melchert-Dinkel, had convinced Nadia that the only way to release herself from her depression was to commit suicide.⁷⁹ On March 10, 2008, Nadia drowned herself in Ottawa’s Rideau River.⁸⁰

Celia Bay, a retired school teacher suffering from depression had found Cami on a similar social networking site.⁸¹ After reading some of Cami’s posts to children suffering from

⁷³ *Id.* at 91.

⁷⁴ *Id.* at 92.

⁷⁵ *Id.*

⁷⁶ ANDREWS, *supra* note 2, at 92.

⁷⁷ *Id.*

⁷⁸ *Id.*

⁷⁹ *Id.* at 92-93.

⁸⁰ *Id.* at 93-94.

⁸¹ ANDREWS, *supra* note 2, at 92-93.

depression, Celia realized that something was wrong.⁸² Cami, a.k.a. Melchert-Dinkel, had been telling depressed children that he would enter into suicide pacts with them, where they would both kill themselves together on web camera.⁸³ Celia brought all of the evidence and suspicions she had gathered on Cami, whom she believed to be Melchert-Dinkel, to the police.⁸⁴ When the police finally investigated Celia's claims, they discovered that Cami was in fact Melchert-Dinkel and had pressured dozens of people into committing suicide, including Nadia.⁸⁵

Nadia's parents wanted Melchert-Dinkel to be brought to justice for his connection to Nadia's suicide.⁸⁶ However, many places will not hold a person liable for another's suicide unless he had provided the physical means by which Nadia killed herself or participated in the physical act of Nadia killing herself.⁸⁷ Melchert-Dinkel argued that he had neither of the actions required for him to be charged with assisting in Nadia's suicide.⁸⁸ Furthermore, Melchert-Dinkel argued that his words were protected under the First Amendment.⁸⁹ However, under the Constitution the government can penalize speech on the basis that it will incite or cause imminent harm to another individual.⁹⁰ In order to prosecute Melchert-Dinkel, a judge would

⁸² *See id.* at 93.

⁸³ ANDREWS, *supra* note 2, at 93.

⁸⁴ *Id.* at 93-94.

⁸⁵ *Id.*

⁸⁶ *Id.* at 94.

⁸⁷ ANDREWS, *supra* note 2, at 94.

⁸⁸ *Id.*

⁸⁹ *Id.*

⁹⁰ *Id.* at 95.

have to find that his chat room conversations went beyond normal speech and incited imminent harm or danger.⁹¹

Judge Neuville rejected Melchert-Dinkel's First Amendment argument to free speech and pointed out that the First Amendment is not absolute.⁹² Furthermore, Judge Neuville pointed out that Melchert-Dinkel's "encouragement and advice imminently incited the suicide of Nadia" and labeled his advice as "lethal advocacy."⁹³ Judge Neuville compared Melchert-Dinkel's words to the specific category of unprotected speech known as "fighting words" and "imminent incitement of lawlessness."⁹⁴ In May 2011, Judge Neuville levied a very peculiar sentence on Melchert-Dinkel.⁹⁵ Melchert-Dinkel would serve 320 days in prison, "plus an additional two days on the anniversaries of both victims [Nadia and Mark Drybrough] each year until 2021."⁹⁶

This particular case is a warning of the possible harms that can be perpetuated through social media sites. In order for justice to be brought to the Web, freedom of speech needs to be limited when it is likely to cause imminent harm to another individual.⁹⁷ The author proposes that these limits should not only apply to the individuals on the social networks, but "to any social networks or websites that act as co-conspirators."⁹⁸

⁹¹ *Id.*

⁹² ANDREWS, *supra* note 2, at 96.

⁹³ *Id.*

⁹⁴ *Id.*

⁹⁵ *Id.* at 97.

⁹⁶ *Id.*

⁹⁷ ANDREWS, *supra* note 2, at 110.

⁹⁸ *Id.*

E. Privacy of Place

In another bizarre incident, Lower Merion School District had issued 2,300 free laptops to its teachers and students.⁹⁹ Unbeknownst to the students or teachers, the free laptops were transmitting screenshots and pictures to the School District's Information Services Department for review.¹⁰⁰ When students and teachers found out that they were being spied on in their homes, they were furious.¹⁰¹

Blake, one of the students who had been spied on, along with his parents found out the hard way that no federal laws have caught up with the regulation of social networks and digital devices.¹⁰² U.S. Attorney Zane Memeger specifically stated, "For the government to prosecute a criminal case, it must prove beyond a reasonable doubt that the person charged acted with criminal intent. We have not found evidence that would establish beyond a reasonable doubt that anyone involved had criminal intent."¹⁰³ With criminal prosecution unlikely to happen, Blake's family decided to take their case to the civil courts.¹⁰⁴ Three months after Blake's lawsuit had been filed, the school district finally agreed to stop the remote activation of student laptops.¹⁰⁵ Additionally, the district promised to destroy all of the photos that had been taken after the

⁹⁹ *Id.* at 111.

¹⁰⁰ *Id.*

¹⁰¹ *Id.* at 111-12.

¹⁰² ANDREWS, *supra* note 2, at 113.

¹⁰³ *Id.*

¹⁰⁴ *Id.*

¹⁰⁵ *Id.* at 115.

students and their parents had a chance to look at them.¹⁰⁶ In October 2010, months after the lawsuit had been filed, the school district decided to settle the lawsuits outside of court.¹⁰⁷

This case is a prime example of how laws can lag behind technological innovation. Privacy laws need to be updated in order to protect individuals in their homes from remote spying through electronic devices. Author Lori Andrews, advocates for declaring a right to privacy while using social networks in order to protect our privacy from the intrusions of third parties.¹⁰⁸

F. Privacy of Information

Employers, schools, and many other institutions are continually seeking more information from social media sites in order to make more informed decisions about people.¹⁰⁹ However, the small glimpses of an individual's life that these social networking sites can offer are causing the proliferation of false and misleading judgments.¹¹⁰ Leaks from social media sites have "led to people divorcing, being fired, being denied admission to college, and committing suicide."¹¹¹

¹⁰⁶ ANDREWS, *supra* note 2, at 115.

¹⁰⁷ *Id.* at 115-16.

¹⁰⁸ *Id.* at 118-19.

¹⁰⁹ *Id.* at 122.

¹¹⁰ *See id.* at 122-23.

¹¹¹ ANDREWS, *supra* note 2, at 122.

In one particularly intrusive and saddening case, the gory images of an 18-year-old girl in a fatal car accident spread across the Internet causing irreparable harm to the family.¹¹² The gruesome pictures disbursed across the Internet after a dispatcher at the precinct that handled the accident, sent the pictures to his private email.¹¹³ Unable to find peace and escape the gruesome pictures, the girl's parents filed a lawsuit against the California Highway Patrol that managed the accident.¹¹⁴ The case went all the way to the California Court of Appeals before the officers were found to have violated their fiduciary duties to the family.¹¹⁵ The California Court of Appeals had found that the officers handling the accident owed the young girl's family a duty of care not to place the accident's photos on the Internet.¹¹⁶ The one positive thing to come out of this case was that the gate had now been open for legal action in future cases involving the invasion of privacy connected with the Internet.¹¹⁷ Private images such as the aforementioned deceased girl's pictures should not be allowed to be disseminated without legal repercussions. Recognizing an individual's legal right to privacy could help prevent future dissemination of private information.¹¹⁸

G. FYI or TMI?: Social Networks and the Right to a Relationship with Your Children

Social media is changing the way courts and investigators gather information.¹¹⁹

Postings on social media sites are being used as evidence in custody proceedings and divorces.¹²⁰

An American Academy of Matrimonial Lawyers poll found that 81% of divorce attorneys have seen an increase in the use of social networking evidence when couples divorce.¹²¹

¹¹² See *id.* at 133-34.

¹¹³ ANDREWS, *supra* note 2, at 133.

¹¹⁴ *Id.* at 134.

¹¹⁵ *Id.*

¹¹⁶ *Id.*

¹¹⁷ *Id.*

¹¹⁸ See ANDREWS, *supra* note 2, at 135.

¹¹⁹ *Id.* at 137.

¹²⁰ ANDREWS, *supra* note 2, at 137.

¹²¹ *Id.*

Attorneys involved in custody battles are also seeing a significant increase in the use of social networking posts as evidence in cases.¹²² Both men and women are losing custody of their children due to the irresponsible posts they make on their social media websites.¹²³ Courts are continually admitting evidence from social networks to help determine which parent will retain child custody.¹²⁴ Evidence such as pictures of parents drinking on Facebook are being used to argue that parents are unfit to care for their children.¹²⁵ The use of social network posts should only be used when they are directly related to the care of a child.¹²⁶ The overzealous use and magnification of innocent postings can be used to prejudice a judge against an otherwise fit parent.¹²⁷

Parenthood is often considered as one of the “basic civil rights of man.”¹²⁸ Courts have continually reaffirmed that a parent has a fundamental right to determine how to raise their own child.¹²⁹ If courts are allowed to pry into a family’s home life through the use of social networking sites, prejudices can form and the inappropriate denial of parental rights can be proliferated.¹³⁰ Courts have to be careful that they do not unduly prejudice parents when

¹²² See ANDREWS, *supra* note 2, at 137-40.

¹²³ *Id.*

¹²⁴ ANDREWS, *supra* note 2, at 141.

¹²⁵ *Id.*

¹²⁶ *Id.*

¹²⁷ *Id.*

¹²⁸ *Id.* at 140.

¹²⁹ ANDREWS, *supra* note 2, at 140.

¹³⁰ *Id.* at 140-41.

evaluating social posts as evidence.¹³¹ Allowing social posts as evidence in custody battles should be admitted only when there is a direct correlation between the post and the best interest of the child involved.¹³²

H. Social Networks and the Judicial System

Judges, lawyers, and jurors alike are all increasingly using social networking sites to discuss cases and research information.¹³³ In 2008, studies showed that only 15% of attorneys used social networking sites.¹³⁴ Two years later, more than 56% of attorneys had social networking profiles.¹³⁵ The increased use of social network sites by attorneys and judges have in some cases led to suspicions of prejudice and conflict of interests.¹³⁶ In 2009, Judge Saffold was removed from a case when it was discovered that she had potentially made prejudicial statements against an attorney in a case she was presiding over.¹³⁷

Jurors' use of social networking sites have also increasingly led to mistrials and overturned judgments.¹³⁸ In 2009, a single court had 600 potential jurors dismissed when they

¹³¹ *Id.* at 141.

¹³² *Id.*

¹³³ *See* ANDREWS, *supra* note 2, at 149-59.

¹³⁴ ANDREWS, *supra* note 2, at 153.

¹³⁵ *Id.*

¹³⁶ *See* ANDREWS, *supra* note 2, at 149-59.

¹³⁷ ANDREWS, *supra* note 2, at 151.

¹³⁸ *Id.* at 154.

had mentioned that they had done prior research about individual cases.¹³⁹ Technology and social networking sites can allow jurors to easily gain access to outside information which can prevent a defendant from a fair trial.¹⁴⁰ In one particular case, a juror used his smartphone to look up a key legal term in a manslaughter trial.¹⁴¹ Only after the defendant had been convicted, did the external research done by the juror emerge.¹⁴² The defendant was granted a new trial with the appellate court stating,

“Although here we confront new frontiers in technology, that being the instant access to a dictionary by a smartphone, the conduct complained of by the appellant is not at all novel or unusual. It has been a long-standing rule of law that jurors should not consider external information outside the presence of the defendant, the state, and the trial court.”¹⁴³

Judges and lawyers have long been held responsible when using social networks in ways that can negatively impact cases.¹⁴⁴ Jurors have also begun to be penalized for ignoring instructions and conducting external research.¹⁴⁵ In order for all people to be afforded fair trials,

¹³⁹ *Id.*

¹⁴⁰ *Id.*

¹⁴¹ *Id.* at 156.

¹⁴² ANDREWS, *supra* note 2, at 156.

¹⁴³ ANDREWS, *supra* note 2, at 156.

¹⁴⁴ *Id.* at 158.

¹⁴⁵ *See* ANDREWS, *supra* note 2, at 158-59.

judges, lawyers, and jurors must be disciplined for prejudicial use of social networks and technology.¹⁴⁶

I. The Right to a Fair Trial

The increased use of social network sites as evidence in criminal cases has many people questioning the validity of that evidence. In Martinsburg, West Virginia, a robber had checked his Facebook on the victim's computer and then left the computer with his Facebook page still open.¹⁴⁷ Officers were easily able to identify and find the suspect from his Facebook page.¹⁴⁸ In this case it turns out that the use of a social network site as evidence was beneficial. However, there are many cases where social networking sites have been used to frame the wrong person or create prejudicial thoughts against potential suspects.¹⁴⁹

“A [recent] survey by the International Association of Chiefs of Police of 728 law enforcement agencies ... found that 62% of the agencies used social networks in criminal investigations.”¹⁵⁰ In some of the more bizarre cases, thieves have been identified after having posted pictures of themselves on social networking sites with the stolen goods.¹⁵¹ Additionally,

¹⁴⁶ ANDREWS, *supra* note 2, at 159.

¹⁴⁷ *Id.* at 161.

¹⁴⁸ *Id.*

¹⁴⁹ *See id.*

¹⁵⁰ ANDREWS, *supra* note 2, at 162.

¹⁵¹ *Id.*

Robert Petrick's conviction for murdering his wife was based off evidence gleaned from his computer's search history on how to kill his wife and where to dump the body.¹⁵²

Despite the many cases that have been solved through the use of social networking sites, the current uses of these sites tramples on individuals' Fourth Amendment rights.¹⁵³ The Fourth Amendment was meant to protect individuals' privacy and to prevent unreasonable searches and seizures of property.¹⁵⁴ Officers need some individualized suspicion that an individual has committed a crime before they can search them.¹⁵⁵ The use of aggregate data from social networking sites completely sidesteps the element of individualized suspicion and can cause discrimination.¹⁵⁶ In a particular case, an African American man was searched at an airport based on aggregate data that shows drug runners carry little luggage and appear to be nervous.¹⁵⁷ The man was found to have drugs on him, but a dissenting judge argued that the search was improper.¹⁵⁸ The judge proclaimed that he himself is sometimes agitated when he flies, but he is never searched because he is white.¹⁵⁹

Judges, prosecutors, and officers need to be careful when verifying the validity of information obtained on social networking sites. The author argues that social networks should not be accessed for evidence unless there is an individualized suspicion that that person has

¹⁵² *Id.*

¹⁵³ See ANDREWS, *supra* note 2, at 162-63.

¹⁵⁴ ANDREWS, *supra* note 2, at 163.

¹⁵⁵ *Id.*

¹⁵⁶ *Id.*

¹⁵⁷ *Id.*

¹⁵⁸ *Id.*

¹⁵⁹ ANDREWS, *supra* note 2, at 163.

committed a crime.¹⁶⁰ Furthermore, when judges allow social networking evidence to be admitted, the reliability, authenticity, and relevance of the evidence must be taken into consideration.¹⁶¹

J. The Right to Due Process

The thoughtless speed in which social networking sites change their privacy policies has caused harm to many of their users.¹⁶² When Facebook changed its privacy policies, many Iranian-Americans who opposed Iran's policies received threats.¹⁶³ The families of these Iranian-Americans still in Iran were arrested and also threatened.¹⁶⁴

Currently, users of social networking sites like Facebook do not receive adequate warning of the repercussions their postings can cause.¹⁶⁵ Additionally, users of social networking sites are not receiving adequate notices of when these sites change their policies.¹⁶⁶ Users on social networking sites should be told well in advance of policy changes that could potentially affect their lives and privacy.¹⁶⁷ Furthermore, no policy change should be

¹⁶⁰ ANDREWS, *supra* note 2, at 171.

¹⁶¹ *Id.*

¹⁶² *See id.* at 173.

¹⁶³ ANDREWS, *supra* note 2, at 173.

¹⁶⁴ *Id.*

¹⁶⁵ *Id.* at 175.

¹⁶⁶ *Id.* at 182-83.

¹⁶⁷ *Id.* at 182.

implemented without a user's explicit consent and knowledge of what the policy changes entail.¹⁶⁸

III. RECOMMENDATIONS

The demand for greater privacy and protection on social networking sites will lead to better legal regulation of the Internet.

A. *Slouching Towards a Constitution*

The outcry for greater privacy comes as no surprise with the way social networking sites currently mine and sell our data without users' consent. Social networking sites such as Facebook provide users with ample opportunities to express one's individuality and thoughts.¹⁶⁹ However, without some more regulation on how these sites use our data, the value of joining these sites will be greatly reduced.¹⁷⁰ As more users become aware of how their privacy is being taken away, there will hopefully be a greater demand to take back their fundamental rights. Social network and Internet users need to band together and apply our Constitutional rights of privacy and expression to not only offline actions, but to online activities as well.¹⁷¹

¹⁶⁸ ANDREWS, *supra* note 2, at 182.

¹⁶⁹ *See id.*

¹⁷⁰ ANDREWS, *supra* note 2, at 188.

¹⁷¹ *See id.*

IV. CONCLUSION

In order to protect our fundamental rights of privacy and freedoms of expression and speech, Lori Andrews purposes that all Internet and social networking users adopt a Social Network Constitution.¹⁷² Among the numerous principles and ideologies described throughout her book, the most important points can be summed up in the ten rights and freedoms of her Social Network Constitution.¹⁷³

The first right is the right to connect.¹⁷⁴ Lori argues that all individuals have a right to connect over the Internet without undue influence from the government.¹⁷⁵ Second, just like in the First Amendment, all individuals have the right to free speech and freedom of expression as long as it does not encroach on the rights of others.¹⁷⁶ Third, users of social networking sites should have the right to privacy of place and information while using those websites.¹⁷⁷ Fourth, users should have the right to have their thoughts and expressions kept private when posting on social sites.¹⁷⁸ Fifth, the image or second self that is created from the information posted on the Internet should be the sole possession of the individual user who created that image.¹⁷⁹ Sixth, evidence should only be collected from social networking sites when there is an individualized

¹⁷² See ANDREWS, *supra* note 2, at 189

¹⁷³ *Id.* at 189-91.

¹⁷⁴ ANDREWS, *supra* note 2, at 189.

¹⁷⁵ *Id.*

¹⁷⁶ *Id.*

¹⁷⁷ *Id.*

¹⁷⁸ *Id.* at 190.

¹⁷⁹ ANDREWS, *supra* note 2, at 190.

suspicion that a user has committed a crime.¹⁸⁰ Seventh, all defendants in court should be judged by an unbiased group of their peers.¹⁸¹ Eighth, users of social networking sites should be given advance notice of site policy changes.¹⁸² Ninth, all users of social networking sites shall not be discriminated against because of data collected on them through networking sites.¹⁸³ Lastly, all social network users shall have the right to associate with whomever they please and to have those associations kept private.¹⁸⁴

DISCLAIMER: This book review is not intended to infringe on the copyright of any individual or entity. Any copyrighted material appearing in this review, or in connection with the *Syracuse Journal of Science and Technology Law* with regard to this review, is disclosed and complies with the fair or acceptable use principles established in the United States and international copyright law for the purposes of review, study, criticism, or news reporting. The views and opinions expressed in the reviewed book do not represent the views or opinions the *Syracuse Journal of Science and Technology Law* or the book reviewer.

¹⁸⁰ *Id.*

¹⁸¹ *Id.* at 191.

¹⁸² *Id.*

¹⁸³ *Id.*

¹⁸⁴ ANDREWS, *supra* note 2, at 191.