Abusive Online Conduct: Discrimination and Harassment in Cyberspace

Andra Gumbus
Sacred Heart University

Patricia Meglich
University of Nebraska at Omaha

Discrimination and harassment that were once committed in real time have now moved to the online environment. Discrimination and harassment on the Internet take many forms and can be more damaging and insidious than the face-to-face forms of abuse. This conceptual paper looks at two types of abusive online conduct that have emerged due to the proliferation of the Internet in our lives: Weblining and cyberbullying. These topics are examined from an ethical perspective with a focus on gender and racial discrimination issues.

INTRODUCTION

Online discrimination by using data footprints to classify and group Internet users based on patterns of Internet activity is becoming more prevalent. Data mining is used to create profiles that can erroneously group users into segments that are not treated equally. In the age of big data, complex analysis extends from marketing and business into the fields of crime, health, retail, and dating. Social networks make it possible to mine large data sets and determine collective online behavior using computer and mathematical models and algorithms. Unfortunately, models can produce correlations which result in oversimplification and inferences based on generalities. This can lead to discrimination in credit or insurance offered, employment decisions, bank loans denied, and denial of health insurance (Lohr, 2012).

Trust is an important part of our online experience where we want to feel safe, confident and secure. However, the very nature of anonymity on the Internet eliminates many mechanisms we use to trust each other. Identities can be conjured or faked, online players are separated in time and space and individuals may feel less accountable because they cannot be easily identified or discovered (Nissenbaum, 2001). Many online sites like Facebook have changed their privacy policies and have issued statements condemning cyberbullying or harassment. Many ISPs prohibit posting offensive content and screen or remove content or discontinue service based on abusive behavior. Policies frequently include phrases regarding refusal to transmit harmful, racially/sexually offensive, vulgar, objectionable, obscene or libelous content (Cohen-Almagor, 2010). While ISPs have a role to play in preventing harassment, they do not control individual online behavior. The Internet offers perils and promises. It has been called the most intimate and uncontrollable medium yet invented (Friesen, 2006).

Cyberbullying and cyber harassment affect more women than men and can involve threats of violence, rape, and other attacks on women (Sheridan & Grant, 2007). Targets are subjected to demeaning

and threatening behavior that can make women vulnerable when they are online. Women have adopted coping mechanisms such as changing their names and refusing to use the Internet or reduce their participation based on fear of future harassment. This can negatively affect career advancement and reduce their ability to socialize and connect using technology. This phenomenon results in men assuming a superior position both personally and professionally and can reduce gender equality in our technology-driven world.

The law does not protect against cyberbullying and women often do not complain or report cyber gender harassment because the public may trivialize the harassment or dismiss it as "just a prank" (Citron, 2009a). Identifying cyberbullying as a form of discrimination can serve to educate and change societal responses by making it unlawful to harass on the Internet. We are at a point where the norms of acceptable online conduct are being challenged and norms are needed to control behavior by regulating and legislating against cyberbullying.

MODERN-DAY REDLINING (AKA WEBLINING)

The term redlining was first used in the 1970s to describe the failure of banks, insurers and other service providers to offer services to residents of the inner city, where a red line was literally drawn on a map to indicate locations where the company would not conduct business. Redlining led to denying home loans to African-Americans regardless of income level and other racially discriminatory practices. Today, the map we use to redline is not a geographical one, but a map of how we navigate the internet, where we go, how much time we spend, what we consume, and what we purchase.

There are no laws that prohibit data aggregation practices that assign individuals to arbitrary groups based on their online behavior. Some have called for a "do not track" law similar to the "do not call" law. A 2008 Consumer Reports poll of 2000 found that 93% felt that internet companies should ask permission before using personal data, and 72% wanted to opt out of online tracking" (Consumers Union, 2008). The European Commission introduced a privacy law that requires web companies to obtain explicit consent before using personal information and gives citizens the power to demand that their data be deleted. All European countries, Canada, Australia, and many Latin American countries have stronger privacy laws than those in the United States. We can only speculate as to the reasons. Is it because privacy is not an issue in the U.S.? Is it because public sentiment favors business over individual rights? Do Americans value the interests of consumers and companies over personal information? Is it because of the significant revenue generated through information trade?

Redlining refers to physical spaces and neighborhoods but discrimination can occur in virtual spaces like Web sites where people are profiled and sorted into groups that are categorized for differential pricing and services. Preferred status would result in favorable interest rates, increased services, and preferential treatment. Marcia Stepanek of Business Week coined the term "weblining" in 2000 when she described how banks ranked their customers and assigned different fees and services based on the rank (Stepanek, Green, Rosenbush, Segd, & Hof, 2000).

This new version of redlining, termed weblining, is defined as "denying people opportunities based on their digital selves." (Andrews, 2012). An online search for information about a medical illness for a friend might result in a denial of insurance based on the assumption that the websurfer had the illness. All websurfers who conduct a similar search would be grouped together and treated as if they have the disease. Insurability, favorable credit card interest rates, and other decisions may be made based upon where someone lives or due to particular online activities. This kind of data aggregation has many negative social ramifications based on assuming individuals in these artificial groups have significant commonalities upon which important decisions may be based.

We now use the term "weblining" in a broader sense than just price discrimination. Weblining refers to the exclusion of classes of consumers from the marketplace based on characteristics of groups not individuals. Individuals in an undesirable group may be denied a loan or credit based on generic characteristics of the group. The decision maker bases the decision on a prediction about the profitability of the members of the group rather than on each individual's unique behavior. People are not treated as

individuals and therefore unjust and unfair practices may prevail. Is this not contrary to what the Internet stands for? Ideally the Internet serves as an equalizer that increases democracy and gives a voice to the powerless. When the Internet is used to redline it creates inequalities and barriers to access. If insurance companies exclude segments of the marketplace and limit their sales efforts to the financially well off there may be a disparate impact affecting members of disadvantaged groups. Entire swaths of the population may have difficulty in obtaining reasonably priced insurance, credit, and access to financial and other services. (Chin-Hul & Kleiner, 1999).

At the very least, the quality and validity of information collected on individuals that is relied upon by decision makers may be questionable. Information bits can be taken out of context, may be irrelevant, and might be based on worthless assumptions. This information can be sold to various organizations and move from firm to firm, unchecked for accuracy and appropriateness. This careless disregard penalizes individuals for their predicted, not actual behavior. (http:ecommerce.hostip.info/pages/1078/Weblining-Internet-Redlining)

A lawsuit was filed in 2000 by a resident living in a predominantly black neighborhood that was denied service by an online retailer because of where he lived. The company redlined this neighborhood among others, claiming that their business targets communities with high internet usage, not based on racial or other socio-economic demographics. This is an example of how redlining has spread to cyberspace (Marquess, 2000).

Unfortunately, Weblining captures more than customer related behavior and this is of greater concern to privacy advocates. Companies maintain credit histories, shopping habits, and personal online activity, and other personal preferences such as health, lifestyle, sexual orientation, race, and politics that go beyond what we buy. If this information gets into the wrong hands it can easily lead to social prejudice or worse forms of outcasting and stereotyping. It can also construct a barrier to upward mobility and place the disadvantaged at greater harm as our lives become more intertwined with technology. Using customer relationship management software to grade or rank customers is becoming more common but this can have a negative effect on fairness perceptions if customers recognize the differential treatment and believe it to be unjust (Holbrook & Kulick, 2001).

PRIVACY IN THE TECHNOLOGY AGE

As we continue to share bits of personal information online on sites like Facebook, LinkedIn, Google, email, and shopping sites it naturally raises basic questions about who should have access to this information. Do we sacrifice our privacy for increased convenience? Do we accept increased security at the expense of privacy? (Freidman, 2012).

A four dimensional perspective has historically been used to explain the legal perspective on privacy. The dimensions are:

- Intrusion or physically invading personal solitude or seclusion
- Disclosure of embarrassing private facts
- False public portrayals
- The use of a person's image or identity without permission.

Privacy can be defined in terms of information control and data protection along with the rights we have regarding the collection, processing, and storage of our personal information. The definition has been expanded to include dissemination and use of data. (Phelps, Nowak, & Ferrell, 2000). Control relates to whether or not the individual is provided an opt-in or opt-out choice for various uses of their information. Most firms do not provide details on how information will be collected or used. Social networking platforms are no different in failing to delineate possible uses of information gathered on a site.

Privacy is being redefined in the age of technology. Nissenbaum (2004) cites public surveillance as one of the most controversial challenges to privacy. She proposed a new benchmark for privacy termed "contextual integrity". This means that the context dictates the appropriateness of information gathering

and dissemination and the norms of distribution in that context. Norms of appropriateness dictate what information about individuals is appropriate to reveal in a certain context. Norms of flow or distribution of information govern the movement or transfer of information from one party to another. A privacy violation occurs whenever one of these norms is violated.
Three principles regarding privacy are proposed (Nissenbaum, 2004).

- Limiting surveillance of citizens and use of information about them. This first principle deals with the imbalance of power between individuals and large corporations and the fact that it is easier for record keeping systems to affect people than vice versa.
- Restricting access to sensitive, personal or private information. This second principle focuses on standards of confidentiality and highlights the notion that sensitive information about habits, actions, and relations is private and should be protected.
- Curtailing intrusions into places deemed private or personal. This third principle is founded on the premise that certain spaces or places (such as one's home) are sacred and should not be violated or intruded upon.

These principles have come under debate and the proliferation of technology in our lives has led to many grey areas regarding expectations of privacy. Our privacy is continually eroding as we rely more frequently on the Internet for our personal and professional lives. For many of us the trade-offs are worth it. Individuals may accept less privacy for more medical care, ease of financial transactions, easier shopping, and for the pleasure of social networking with friends. We have given up privacy under threats of safety and security and in many instances when we say our privacy has been invaded it is in reality a breach of security. Identity theft and the misuse of social security numbers are examples of a security breaches that can result in financial harm. Dyson distinguishes these from a breach of privacy where the harm a person feels is more personal and subjective. She argues that people should have control over what they disclose because disclosure is a personal and individual preference and privacy cannot be legislated nor defined as a one size fits all. Our expectations of privacy change over time and who we want to see our personal information and what information they should see changes over time (Dyson, 2008).

On February 23, 2012 President Obama outlined a set of privacy principles that provide consumers a one-click process to inform Internet companies whether they want online activity tracked (Wyatt, 2012). The administration seeks a win-win situation where consumers will have privacy and electronic commerce will also grow. Obama stated, "by following this blueprint, companies consumer advocates and policy makers can help protect consumers and ensure the Internet remains a platform for innovation and economic growth." (Wyatt, 2012). Congress will have to enact legislation and the browser companies will have to agree to new standards; a process which may take years. Then the Commerce Department will develop enforcement policies for a Consumer Privacy Bill of Rights to include individual control, transparency, security, access, accuracy and accountability (Wyatt, 2012).

DATA MISUSE BY MARKETERS

The proliferation of sharing encouraged by social networking sites is eroding our definition and sense of privacy and blending the private domain with the public domain. "As the scope of sharing personal information expands from a few friends to many sundry individuals grouped together under the Facebook label of 'friends,' disclosure becomes the norm and privacy becomes a quaint anachronism." Facebook's younger members are comfortable sharing while older members are not used to the levels of personal disclosure. Consumers have the option to block cookies that capture data by using features on the browser but most do not know how and do not block (Milne, 2000).

When we shop online we are usually unaware of how our personal information will be used nor do we understand the terms of release of information and cannot retract permission once given. There is not a fair exchange between business and consumer. This rampant misuse of information leads to significant privacy-related challenges in consumer data collection and use. Fundamental questions regarding the purpose and scope of data collection, informed consent, user control, and the like must be resolved.

Appropriate norms regarding consumer data collection for advertising and marketing purposes must be established. Standard metrics for utilizing consumer data for advertising purposes must be developed. A viable privacy standard must be agreed on, and the practical realities of a market where numerous metrics and privacy standards coexist must be addressed. Further, a legal concern exists about whether a consumer's online behavior should be viewed as speech or property.

Analytic software allows marketing firms to sort customer information into patterns in order to segment the customer base. Web-generated data can be collected from registration forms, online transactions, and other clickstream records. Marketers use clickstream data to analyze paths, shopping carts, key word searches, and entry and exit points. Decision tree models are used to sort customers into groups to make predictions about their behavior. Other tools such as market basket analysis let retailers know what items are bought together to enable personalized communication to the consumer. This aggregating or grouping of individuals into categories may be efficient for marketers, but the "group profile" may not be accurate for any individual in the group. This is the crux of the ethical issue with behavioral advertising – there are consequences that flow from the errors made in assigning an individual to a profile group that may have deleterious effects on his or her purchasing power.

Price discrimination occurs when the same item is sold to different people at different prices. Classifying customers into groups results in differential treatment of individuals based upon group attributes. A customer in the "desirable" group may be given a lower price than one in the "undesirable" group who may be offered the product at a higher cost, or perhaps not at all. Individuals in lower income and socio-economic groups can experience discrimination in the marketplace based on stereotypes and assumptions. This conflicts with the notion of equality and egalitarianism and results in charging the buyer the highest price they are willing to pay for an item. It may serve as a mechanism to cull the customer list. Less desirable customers may cease doing business with the firm. Customer relationship management and "ranking" customers into profitability tiers is nothing new. It has been practiced by banks, credit card companies, airlines and most service providers for decades. However, the sheer magnitude of the information available regarding online activity has grown exponentially and presents a greater risk of unfavorable treatment to the disadvantaged. Legal and consumer backlash can result from charging different prices to customers based on how profitable they are (Iyer, 2002).

Behavioral advertising involves tracking a consumer's online activities, including searches conducted, Web pages visited, and the content viewed, in order to deliver advertising targeted to that individual. The House Committee on Energy and Commerce solicited privacy standards from 33 cable and Internet companies to provide information on behavioral targeting. Regulators and privacy advocates are concerned because advertisers are becoming more sophisticated about tracking online activities. Some feel that electronic privacy legislation is needed to curb controversial new techniques like deep packet inspection. Marketers claim to protect privacy by maintaining individual anonymity and avoiding sensitive information such as HIV status. The problem intensifies due to the ever changing ways of tracking and handling data. The Federal Trade Commission has proposed that companies provide consumers control to opt out of tracking and to notify consumers if they change the way data is used or shared (Clifford, 2008). Even if profiling and tracking are acceptable to the customer they may not agree to the use of their data by advertisers who attempt to manipulate them to purchase things they did not intend to buy. Profiling can enable firms to avoid certain customers, block their access to information about products, or offer unfavorable terms to undesirable customers (Wiedman, Buxel, & Walsh, 2002). Consumer activists believe that some data capturing and tracking "malevolently manipulate consumers' economic decisions" (Garven, 2002).

Civil liberties groups feel that behavioral targeting is harmful. Others believe in self-regulation citing that it is not clear if consumers are being harmed. The Online Privacy Alliance and the Network Advertising Initiative asks members to follow guidelines on consumer notification and de-identifying information. A comprehensive federal privacy law may be the answer. A survey of 1000 users was conducted to determine concerns about advertisers tracking Web movement and targeting ads. Thirty nine percent of respondents were strongly opposed and only six percent strongly agreed with the practice (Clifford, 2008). During the 2012 presidential election campaign microtargeting was used to customize

ads to registered voters by analyzing consumer behavior both online and off. Microtargeting allows campaigns to focus specific messages to particular groups of voters. Two people in the same household could get two different messages due to the sophistication of this technique (Vega, 2012). Critics claim that this amounts to social discrimination because only registered voters get messages. Political redlining occurs when segments of the population do not receive campaign communication because they do not fit the profile of a sympathetic voter.

CYBERBULLYING AND HARASSMENT

Cyberbullying is defined as willful and repeated harm inflicted through the medium of electronic text and attacks victims by degrading, threatening and/or sexually explicit messages and images conveyed using web sites, instant messaging, blogs, chat rooms, cell phones, web sites, email, and personal online profiles (Shariff, 2006). Many terms are used to describe the phenomena including electronic bullying, e-bullying, SMS bullying, mobile bullying, online bullying, digital bullying and Internet bullying (Privitera & Campbell, 2009). The definition of bullying usually involves intention, repetition, and power imbalance. Anonymity and publicity are additional dimensions used to define cyber-specific bullying (Nocentini, Calmaestra, & Menesini, 2010). Confederates can be recruited to contribute hateful remarks or stream malicious messages. Cyber bullies are hard to detect and identify which gives them power and control over their targets (Li, 2006).

Cyberbullying became a household word in 2003 with the suicide of Ryan Halligan due to an online prank from other 13 years olds. In 2006, news of the suicide of 13-year-old Megan Meier (who was harassed by Lori Drew on MySpace posing as "Josh Evans") shocked and alarmed parents who allowed Internet use. The Internet poses many risks to children and teens but perhaps the greatest challenge is the ability to be anonymous online. Studies have found that between 8% of teenagers and 18% of middle school children have been victimized by cyber bullies – with girls being most prevalent as both bullies and targets (Winchester, 2009, Wagner, 2008).

The phenomenon of cyberbullying is alive and well in workplaces as well as in schools. A study of manufacturing workers showed that the most frequently cited negative acts using technology were withholding information by email (55 percent) or phone (37 percent) and being targets of gossip spread by phone (38 percent). Thirty eight percent also reported being subjected to email messages containing allegations or being assigned an unmanageable workload (Privitera & Campbell, 2009). In a study conducted in three European countries, four categories of behavior were classified as cyberbullying. In a study of the severity of types of cyberbullying 1,092 Italian adolescents reported that less severe acts were silent or prank calls and insults using instant messaging were less severe than sending unpleasant pictures, photos on web sites, phone pictures and videos of intimate or violent scenes. Moderate to high levels of severity were reported for nasty text messages, rude emails, and insults on web sites, chatrooms and blogs (Menesini, Nocentini, & Calussi, 2011). Cyberbullying behaviors such as flaming, harassment, denigration, impersonation, outing, trickery, exclusion, and cyber stalking were classified into the following four groups - written-verbal behaviors, visual behaviors, exclusion, and impersonation.

Men can be targets of cyberbullying, but the majority of targets are women according to statistics compiled by a nonprofit organization Working to Halt Online Abuse. The 2007 survey showed that 61 percent of targets were women and 21 percent were men. The 2006 results showed that 70 percent of targets were women. Between 2000 and 2008, 73 percent of the 2,519 individuals targeted were women and 22 percent were men (Working to Halt Online Abuse, 2006). The Stalking Resource Center of the National Center for Victims of Crimes reports that female targets are attacked by males in 60 percent of online harassment cases (Petrozzo & Stapp, 2008). Clearly, the preponderance of targets in cyber harassment and stalking cases are women which indicates that sex discrimination has migrated to the internet.

Blog comments regarding women reveal threats of sexual violence, treating women as sexual objects, and using stereotypical language that demeans women (Valenti, 2007). Fortunately, a group called Anonymous works to shut down message boards and sites that attack women on the Web or gender harass

women on the Web. Online harassment mirrors harassment that occurs face to face in the workplace. To escape harassers and bullies, female employees transfer jobs or leave their employment. Women respond in similar ways online by editing blogs or leaving websites to avoid abuse. This can negatively impact their professional and career goals.

Cyber harassment of women is trivialized and therefore not taken seriously by law enforcement. A 1999 Department of Justice report on cyberstalking showed that the majority of claims were not pursued. Officers were not trained to investigate and handle such cases and they advised victims to ignore the harassment. If prosecuted, harassers get minimal punishment such as a fine for a misdemeanor (Citron, 2009b).

Sixty percent of female web designers reported flaming, spamming, harassing posts, belligerent comments, death threats, and sexual harassment when they voiced feminist thoughts on their websites (Kennedy, 2000). Negative reactions include criticism of the website, derogatory insults against participants on the site, attempts to destroy the site by hackers, and threats to personal safety of participants. Most women were angry and frustrated by hostile responses to their postings and over a third reported feeling scared and frightened. In addition to the emotional distress experienced by the web site creators, others who read the negative comments also experienced fear. Some changed their sign-on credentials and identifiers to be more cautious about how they appear on the media. Women who express feminist views are more likely to get negative reactions. Also, sites that promote women in the military or other male dominated professions generate negative feedback. Of course, sites that present men as sexual predators and harassers get negative responses as well as sites that challenge the status quo (Kennedy, 2000). Conversely, others experienced positive reactions including support, encouragement, and a sense of community with other women on the Internet. Thus, the Internet may function as an equalizer that gives voice to women and their issues.

Bullying has moved from the schoolyard to the Internet and media attention has resulted in the adoption of legislation against cyberbullying in five states as of July, 2010. Federal legislation is pending (Hinduja & Patchin, 2010). The Megan Meier Cyberbullying Prevention Act has been proposed to make it a crime to "cause substantial emotional distress to a person using electronic means to support severe, repeated, and hostile behavior." Punishment may include fines and up to two years of imprisonment (Meredith, 2010). Under Title VII of the Civil Rights Act an employer's lax attitude toward email and Internet abuse can contribute to a hostile environment by allowing racial or sexual content to be distributed or failing to monitor work to prevent harassment (Panko & Beh, 2002). The Communications Decency Act prohibits the use of telecommunications devices to harass or annoy, including email, pictures, text, or faxes. The employer may be liable if they knew about or tolerated the conduct (Whitman, Townsend, & Alberts, 1999).

Organizations are increasingly monitoring employees' online activity to protect themselves against racial and/or sexual harassment claims. In a survey conducted by the American Management Association 63 percent of employers reported monitoring Internet use, 47 percent store or review emails, 15 percent view employees by video, 12 percent record phone messages and 8 percent review voice mail of employees in order to reduce risk of litigation or civil rights violations (Sinrod, 2001). Companies should adopt email and Internet use policies and inform employees of their right to review and monitor emails (Towns & Johnson, 2003).

CONCLUSION

Social media may be regarded as a portal rather than a pitfall (Klass, 2012). Comparisons are made to the introduction of the telephone and related fears of dangerous outcomes to society, "men would be calling women and making lascivious comments, and women would be so vulnerable, and we'd never have civilized conversations again." (Klass, 2012). Perhaps a more balanced approach to social media and the Internet is needed. Considered as a rite of passage for youth, (Klass compared it to driving a car) it is neither good nor bad, but neutral. Young adults experience social media as part of the passage to adulthood and they learn how to socialize, test their independence, and learn about the world as they gain

communication skills. Parents need to manage the social development of their offspring and reduce the potential dangers or mistakes made online and serve as guides to use of the media. Social media is a platform that can facilitate the transition from childhood to independent adulthood. The technology can be seen as beneficial in that process. While the seriousness of cyberbullying and abuse on the Internet are very real problems, youths perceive bullying as "drama" while adults label it "bullying" (Klass, 2012).
Problems with consumer privacy are frequently cite in the media targeting Google, Apple, Facebook, Amazon, Sony and other internet services that have failed to build privacy safeguards into the design of their products. Privacy gets attention when a mishap occurs or the FTC enforces breaches or invasions. We cannot assume that consumers will simply stop using technology if they fear for their right to privacy. Although legislation is not ideal for anyone, the current default to self-regulation is clearly not working. "Companies need to look at privacy issues in terms of consumer needs, baking in privacy by design when building apps, so you're not trying to do it afterwards" (Bilton, 2012).

Weblining will only increase as computing affords companies the ability to predict human behavior even if it is not accurate at the individual level. Unfortunately we are often not aware of our rankings or profiles and we cannot verify their accuracy. Do we want a marketplace where only customers with a top tier profile get the best deals and best service? Are loyalty cards and their inherent benefits a form of snobbery? These are ethical questions that are not easily answered.

At a minimum, consumers should be informed of what data is tracked and how it is tracked, stored, and shared and should be given the choice to opt out if desired. We could then say that the practice was universalized and ethical as opposed to market practices that focus primarily on profitability for the firm at the expense of the consumer. Weblining is the antithesis of the difference principle that suggests that we benefit the least well off and give preferential treatment to the impoverished. Let's hope that future federal legislation affords a Consumer Bill of Rights that ensures fair and equitable treatment.

Cyberbullying should be attacked on legislative, educational, and organizational fronts. In addition to legislation discussed in this article, education is critical to ensure that targets know how to respond in an ethical and effective way to cyberbullying. The Student Internet Safety Act of 2009, the Adolescent Web Awareness Requires Education Act (AWARE), and the SAFE Internet Act are ways to fund education and research on cyberbullying and how to prevent it (Meredith, 2010). Web Wise Kids teaches kids ways to safely and effectively react to harassment online. Since technology continually evolves it is timely to respond with education and awareness rather than to wait for legislative solutions that can be slow and reactive as opposed to proactive. Others believe victims should ignore the abuse and the provocation will cease if the bully gets no reaction. Or, write a limited response that is direct and curt stating that you find the communication offensive and will not tolerate it (Richman & Iachan, 2010).

Discrimination and harassment are societal problems that must be addressed regardless of the medium used to negatively impact a segment of the population and cause personal and professional harm. The causes and solutions to these social ills remain the same regardless of the medium used to harass or discriminate.

REFERENCES

Andrews, L. (2012). Facebook is Using You. *New York Times*, February 5.

Bilton, N. (2012). Disruptions: And the Privacy Gaps Just Keep on Coming. *New York Times*, February 19.

Chin-Hul L.J. & Kleiner, B. (1999). Discrimination in the Insurance Industry. *Equal Opportunity International,* 18, (5/6), 62-69.

Citron, D.K. (2009a). Law's Expressive Value in Combating Cyber Gender Harassment. *Michigan Law Review,* 108, 373- 414.

Citron, D.K. (2009b). Cyber Civil Rights. *Boston University Law Review,* 61, 69 -75.

Clifford, S. (2008). Web Privacy on the Radar in Congress. *New York Times*, August 10.

Cohen-Almagor, R. (2010). Responsibility of and Trust in ISPs. *Knowledge Technical Policies,* 23, 381-397.

Danna, A. & Gandy, O. (2002). All that Glitters is Not Gold*. Journal of Business Ethics,* 40, (4) 373-387.

Dyson, E. (2008). Reflections on Privacy 2.0. *Scientific American,* September, 50-55.

Friedman, B. (2012). Privacy, Technology and Law. *New York Times,* January 24.

Friesen, G.B. (2006) The Peril and Promise of Internet-enabled Information Flow. *Consulting to Management,* 17, (2), 37-41.

Garven, J. (2002). On the Implications of the Internet for Insurance Markets and Institutions. *Risk Management and Insurance Review,* 5, (2), 105-117.

Hinduja, S. & Patchin, J. (2010). State Cyberbullying Laws: A Brief Review of State Cyberbullying Laws and Policies. Cyberbullying Research Center (July, 2010). Retrieved from http://cyberbullying.us.

Holbrook, R. & Kulick, C. (2001). Customer Perceptions of Justice in Service Transactions: The Effects of Strong and Weak Ties. *Journal of Organizational Behavior,* 22, (7), 743-757.

Iyer, G. (2002). Linking Web-based Segmentation to Pricing Tactics. *Journal of Product and Brand Management,* 11, (4), 288-302.

Kennedy, T. (2000). An exploratory study of feminist experiences in cyberspace. *Cyberpsychology and Behavior,* 3(5), 707-719.

Klass, P. (2012). Seeing Social Media More as Portal Than as Pitfall. *New York Times,* January 10.

Li, Q. (2006). Cyberbullying in Schools: A Research of Gender Differences. *School Psychology Internationa*l, 27, (2), 157–170.

Lohr, S. (2012). The Age of Big Data. *New York Times*, February 12.

Marquess, K. (2000). Redline may be Going Online. *ABA Journal,* 86, (8), 80-83.

Menesini, E., Nocentini, A., & Calussi, P. (2011). The Measurement of Cyberbullying: Dimensional Structure and Relative Item Severity and Discrimination. *Cyberpsychology, Behavior, and Social Networking,* 14, (5), 267-274.

Meredith, J. (2010). Combating Cyberbullying: Emphasizing Education over Criminalization. *Federal Communications Law Journal,* 63, (1), 311-340.

Milne, G. (2000). Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy. *Journal of Public Policy and Marketing,* 19, (1), 1-7.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, 79, 101–139.

Nissenbaum, H. (2001). Securing Trust Online: Wisdom or Oxymoron. *Boston University Law Review,* 81, (3), 107-131.

Nocentini, A., Calmaestra, J., & Menesini, E. (2010). Cyberbullying: Labels, Behaviors and Definition in Three European Countries*. Australian Journal of Guidance and Counseling,* 20, (2), 129-142.

Panko, R. & Beh, H.G. (2002). Monitoring for Pornography and Sexual Harassment. *Communications of the ACM,* 45, (1), 84-87.

Petrozzo, C. & Stapp, S. (2008). To Catch a Predator: How Some Cyber-Agencies Help Victims Fight Back Against Online Aggression. *Syracuse Daily Orange*, January 24.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing,* 19, (1), 27-41.

Privitera, C. & Campbell, M. (2009). Cyberbullying: The New Face of Workplace Bully? *Cyberpsychology and Behavior,* 12, (4), 395-400.

Richman, M. & Iachan, M. (2010). Combating Strategic Incivility in Cyberspace. *American Bankruptcy Institute Journa*l, 29, (6), 26-27.

Shariff, S. (2006). Cyber-hierarchies: A New Arsenal of Weapons for Gendered Violence in Schools. In C. Mitchell & F. Leech (Eds.), *Combating Gender Violence in Schools.* London: Trentham Books.

Sheridan, L.P. & Grant, T. (2007). Is Cyberstalking Different? *Psychology, Crime and Law*, 13, 627–637.

Sinrod, E. (2001). Eyeing Electronic Surveillance in the Office. *New York Law Journal,* October 23, 5.

Stepanek, M., Green, H., Rosenbush, S., Zegd, S., & Hof, R. D. (2000). Weblining. *Businessweek*, (3675), 26-34.

Towns, D. & Johnson, M. (2003). Sexual Harassment in the 21st Century—E-harassment in the Workplace. *Employee Relations Law Journal,* 29, (1), 7-24.

Valenti, J. (2007). How the Web Became a Sexist's Paradise. *Guardian,* April 6. Retrieved from http://www.guardian.co.uk/world/2007/apr/06/gender.blogging.

Vega, T. (2012). Online Data Helping Campaigns Customize Ads. *New York Times*, February 21.

Wagner, C. (2008). Beating the Cyberbullies. *The Futurist,* 42, (5), 14-15.

Wiedman, K., Buxel, H., & Walsh, G. (2002). Customer Profiling in E-commerce: Methodological Aspects and Challenges*. Journal of Database Marketing,* 9, (2), 70-185.

Whitman, M., Townsend, A., & Alberts, R. (1999). The Communications Decency Act is not as Dead as You Think. *Communications of the ACM,* 42, (1), 15-17.

Winchester, D. (2009). Cyberbullying on the Rise. *St. Petersburg Times,* March 3.

Wyatt, Edward (2012). White House, Consumers In Mind, Offers Online Privacy Guidelines. *New York Times.* February 23.