# Personal Privacy Has Changed Since The World Wide Web

By Jennifer Gioia

Kent State University

Law for Advertising and Public Relations

December 9, 2017

# Table of Contents

Introduction pg. 2

Legal Analysis pg. 3

Public Relations Analysis pg. 10

Issues and Unanswered Questions pg. 11

Limitations pg. 11

Recommendations pg. 11

Conclusion pg. 13

References pg. 14

## Introduction

Privacy used to belong only to the average citizen, while it was common for public officials, public figures and celebrities to have limited privacy in the spotlight of the public eye. However, thanks to the creation of the World Wide Web about 30 years ago, the life of the normal citizen is no longer private. Anything regarding anyone can now be broadcasted across the Internet for all eyes to see.

"Online privacy covers a broad range of issues often revolving around who has actual access to information about you, who has the legal right to information about you online, and under what circumstances, and for what that information can be used" (Weckerle, pp. 251).

In this paper, I will briefly mention some of the legal standards that have been applied and/or adapted to today's online society regarding privacy through examples of legal cases. I will also touch upon what public relations practitioners need to focus on with today's online legal standards in mind, as well as issues, limitations and recommendations for future research.

## Legal Analysis

"[T]raditional privacy torts are not well-suited to protect users of social media" (Hartzog, pp. 50-51). With the creation of social media, there is an increase in personal information, which leaves users "vulnerable to privacy violations. This vulnerability has raised the question of whether privacy can even exist in online social networks" (Hartzog, pp. 50). Woodrow Hartzog from Cumberland School of Law at Samford University asks, "What information, if any, is private in online social networks? What laws protect this information? Is it reasonable for users to expect privacy in self-disclosed information" (pp. 51)?

Internet users are vulnerable to a wide range of injuries including "excessive government and commercial entity surveillance, breach of confidentiality, misuse of personal information for such things as denial of employment or insurance benefits, damage to reputation, blackmail, loss of anonymity, chilled speech or association, and extreme emotional distress" (Hartzog, pp. 52). To protect an Internet user's privacy, websites, especially social networks, are using contracts in terms of use agreements and privacy policies between the website and the person using the website. With this adaption of traditional law of use agreements and privacy policies applied to the online community, "privacy disputes are increasingly governed by contracts between the user and the website" (Hartzog, pp. 50).

Hartzog explains in his chapter on *Privacy and Terms of Use* in D. R. Stewart's Social Media and the Law some of the many problems preventing traditional torts from protecting the privacy of individuals online. "Many regulatory schemes governing privacy and social media inconsistently apply standards of 'private' information or subjective tests such as one's 'reasonable expectations of privacy.' Approaches that focus on the nature of the information are problematic because personal information is usually not seen as strictly private or public. The

same piece of information collected from social media can be considered sensitive in some circumstances and completely benign in others...Additionally, any law aimed at the suppression of a particular kind of expression is suspect under the First Amendment" (Hartzog, pp. 52).

There is one traditional tort that has been applied to social media that I'd like to highlight known as "the disclosure tort" (Hartzog, pp. 52). "The disclosure tort generally prohibits giving publicly to a matter concerning the private life of another, if the matter publicized is of a kind that would be highly offensive to a reasonable person and is not of legitimate concern to the public" (Hartzog, pp. 52). According to Hartzog, the disclosure tort was criticized before the creation of the Internet, and it still has its flaws when applied online, including "a difficulty in deciding when expectations of privacy are reasonable" as well as when First Amendment concerns take precedence over privacy, rendering it useless in protecting the privacy of an individual on social media (pp. 53).

The 1989 case *Florida Star v. B.J.F.*, the U.S. Supreme Court "declared that defendants cannot be punished for publishing matters of public significance without the claimant proving that punishment is necessary to advance a state interest of the highest order" (Hartzog, pp. 53).

"The Florida Star, is a newspaper which publishes a 'Police Reports' section containing brief articles describing local criminal incidents under police investigation. After appellee B. J. F. reported to the Sheriff's Department (Department) that she had been robbed and sexually assaulted, the Department prepared a report, which identified B. J. F. by her full name, and placed it in the Department's pressroom. The Department does not restrict access to the room or to the reports available there. A Star reporter-trainee sent to the pressroom copied the police report verbatim, including B. J. F.'s full name. Consequently, her name was included in a 'Police Reports' story in the paper, in violation of the Star's internal policy" (FindLaw).

This "declaration almost guarantees defeat for plaintiffs pursuing claims based on the disclosure tort" (Hartzog, pp. 53). Several scholars claim the disclosure tort has been ineffective since the *Florida Star v. B.J.F.* case, and "[f]or the most part, the privacy torts as defined in the Second Restatement have functioned inadequately and fared poorly in the courts" (Hartzog, pp. 53).

"One scholar has argued that '[a]ttempts to apply traditional public disclosure jurisprudence to online social networking demonstrate the incoherence of this jurisprudence' because the disclosure tort is centered around keeping information from people and social networking is centered around disclosure and sharing of information" (Hartzog, pp. 53).

When dealing with the disclosure tort, it is usually up to judges to "make normative and subjective judgement[s] pertaining to concepts like privacy, public concern, and offensiveness...the tort also calls upon judges to determine what information is 'private' and what information is public or at least 'of public concern' (Hartzog, pp. 53). However, with the creation of the Internet and social networking sites came the evolution of how people communicate, which is quite different than how people communicate in person.

Dr. Joseph Rock, a psychologist at Cleveland Clinic, says, "it's easy for folks to over-share information that they wouldn't normally feel comfortable with sharing to such a large audience if it were done face to face. It's also easy for people lose sight of the fact that often times their responses are not one-on-one conversations, but are seen by many people" (WJHG). Dr. Rock also says, "sharing information and opinions opens the door to negative responses. While some folks are okay with it, others are more prone getting angry or getting hurt feelings" (WJHG).

If the way we communicate and perceive communication is not the same as in-person, the same laws shouldn't be applied to online issues without some adaptation. "It is becoming increasingly clear that the privacy torts, particularly the disclosure tort, are ineffective in many scenarios involving social media" (Hartzog pp. 54). "[T]o distinguish private facts from 'public' information about an individual, courts often look either to the location of the action or to the nature of the subject matter" (Hartzog, pp. 53). The location concept of the disclosure tort cannot apply to online issues; however, the nature of the subject matter can.

Contract law has been adapted and applied to the online world in the form of terms of use between websites and users. "The omnipresent online agreements have come to significantly govern the privacy of Internet users" (Hartzog, pp. 55). Privacy policies can be found in these contracts as well, which explain "how a website will use a visitor's personal information" (Hartzog, pp. 58). These policies are being used more and more on websites "in response to increases in legislation requiring" the disclosure of how users' information is being used, "and as a voluntary measure by websites to appeal to consumers by emphasizing the care with which they treat consumer information" (Hartzog, pp. 58).

These contracts not only protect the privacy of users, but the rights of the website for sharing and selling user information as well. "No law prevents a website operator from sharing or selling information is has lawfully been given, although a website can be held liable for failing to notify its customers of its practice of selling or sharing such information" (Hartzog, pp. 59). The FTC also brings legal "action against entities that mislead consumers about the confidentiality of their personal information" (Hartzog, pp. 63).

However, not many users actually read the terms of use and privacy policies in the contracts they agree upon when signing up with a social network or accessing a website or online

service. “Increasingly often, too, people click away their right to go to court if anything goes wrong,” because they don’t actually read the terms of use and privacy policies (Berreby). David Hoffman, a professor at the University of Pennsylvania Law School who researches the law and psychology of contracts, is “among the legal scholars who believe the no-reading problem isn’t new. After all, he points out, few people read the fine print even when it was literally in print” (Berreby).

“Courts have typically found that terms of use can dispel an expectation of privacy regardless of whether the user actually read the terms” (Hartzog, pp. 61). The case *United States v. Hart* is a great example: “...the government sought and obtained personal information from an email the defendant allegedly used to commit a crime. As part of the email registration process, the defendant consented to terms of service that required the user to acknowledge that his personal information might be disclosed to comply with legal process. The court found that given the defendant consented to the terms of use, ‘it is difficult to conclude that [the defendant] has an actual expectation of privacy in the content of any communications sent or received with his Yahoo! Accounts’” (Hartzog, pp. 61).

In cases like these, it comes down to the terms of the contract users agree with online, no matter if they spent ten seconds or ten minutes reading it over.

These contracts also affects a major advantage the Internet offers users—anonymity. “The right to remain anonymous is a fundamental component of [the people’s] right to free speech, and it applies every bit as much in the digital world as it does in the physical one” (ACLU). However, anonymity can also cause harm, because it can allow users to feel invincible to consequences when no one knows who they are, which has lead governments and corporations

to attempt to "unmask" anonymous speakers "through subpoenas directed at the websites they visit" (ACLU).

The United States government uses a balancing test to determine whether or not to "unmask" an anonymous speaker when they've caused much harm. The court weighs "the interest of the speaker with the interest of the harmed person or entity...One of the factors a court considers when determining whether to compel identity disclosure is 'the expectation of privacy held by the Doe defendants, as well as other innocent users who may be dragged into the case'" (Hartzog, pp. 61).

"While a court's decision whether contract terms establish an expectation of privacy is naturally dependent upon the text of the agreement, interpretation of what a user should expect from the language varies. Some have interpreted the vague nature of online agreements to mean that users naturally expect privacy if the website offers general promises of confidentiality" (Hartzog, pp. 61).

The 2010 case of *McVicker v. King*, "a former employee of the Borough, sought to compel a third-party owner of an internet discussion board to produce information sufficient to identify anonymous authors of certain, relevant posts. Plaintiff argued the identities of the posters may be relevant to impeach defendants' testimony regarding when the determination to terminate plaintiff was first discussed" (K&L Gates). The United States District Court "considered whether to grant motion to compel the disclosure of records that could identify seven anonymous users who commented on a website's message board" (Hartzog, pp. 62).

"Citing First Amendment considerations, the court denied plaintiff's motion to compel" (K&L Gates).

## Public Relations Analysis

As a public relations practitioner in today's online world, you need to go into the workforce with an understanding of your website's terms and conditions as well as the terms and conditions of the social media you use to target and connect with your publics.

You also need to have an understanding of what your publics expect of you. Do they expect you to use their comments on your client's posts as testimony? Do they expect you to ask for permission to use their words?

As a public relations practitioner, you should also be aware of the current laws and regulations for social media use as an organization. If you do use a social media user's comment as testimony, make sure you disclose in the same post as the testimony whether or not they gave you permission, if they're getting paid for it, if they're a "real customer," etc.

If you do attain a social media user as an endorser, the "endorsement must reflect the honest opinion of the endorser and can't be used to make a claim that the product's marketer couldn't legally make" (FTC). How you obtained this endorser, i.e., the connection between you and them, should also be disclosed.

## Issues and Unanswered Questions

"...[T]he invention of the Internet and the spread of online speech have not required the formulation of a new area of 'cyberspace tort law'" (Silver, pp. 23). Why is that?

This paper has brought up many issues and unanswered questions regarding online privacy including how people determine whether privacy has been breached in an online environment. What is considered private, public, or of public concern? What changes have been made and/or should be made to address privacy violation legally on the Internet?

"Unfortunately, privacy in social media remains a vague and constantly evolving concept" (Hartzog, pp. 65). How do we keep up with protecting the right to privacy of individuals online when technology and the way we communicate is always changing?

## Limitations

There are a multitude of traditional laws used to protect the privacy of citizens and large amount of them have been adapted to apply to online scenarios. Since the birth of the Internet, law has attempted to catch up to the movement of technology, and still aims to do so. From this, an innumerable amount of legal cases have come to fruition and it would take more than this paper to cover them all.

Another limitation is that the law still doesn't know how to fully protect all individuals and find that right balance between privacy and public and public concern. It is subjective to each case. Therefore, cannot be generalized or summed up in one paper.

## Recommendations

Barely anyone reads the terms of use and conditions when accessing a social network or other website. Writer for *The Guardian*, David Berreby, brings up the point that "an individual who depends on Google, Facebook or Twitter is not in a position to negotiate her own separate

agreement. Why spend time on a contract you can neither change nor refuse? So the real click-to-agree problem may not be that individuals fail in their duty. It may, instead, be that we have stuck individuals with this impossible duty in the first place. There are, after all, other ways to conceive of our relationships to Google, Facebook, Apple, Amazon and the thousands of other entities that ask us to sign these documents" (Berreby).

Hartzog mentions that "social norms and context play a large role in any such determination, thus standardized rules must be largely displaced with factually-specific determinations. To that tend, the best strategy for social media users is to take a full stock of what context and cues are available when trying to determine whether to disclose personal information or determining if the disclosures of others are private" (pp. 65).

## Conclusion

"Empirical research demonstrated that social media users regularly consider information disclosed on the website as private to some degree. Only a careful consideration of context and cues will help you navigate the grey area of privacy within online communications" (Hartzog, pp. 66). Public relations practitioners are supposed to know their target audiences' wants, needs, motivations and interests. Practitioners should also know what their target audiences expect when it comes to online communication and their privacy online.

## References

ACLU. (2017). Online Anonymity and Identity. ACLU. Retrieved from https://www.aclu.org/issues/free-speech/internet-speech/online-anonymity-and-identity

Berreby, D. (2017). Click to agree with what? No one reads terms of service, studies confirm. The Guardian. Retrieved from https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print

FindLaw for Legal Professionals. (2017). The Florida Star v. B.J.F. FindLaw for Legal Professionals. Retrieved from http://caselaw.findlaw.com/us-supreme-court/491/524.html

FTC. (2017). The FTC's Endorsement Guides: What People Are Asking. FTC. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking

Hartzog, W. (2013). Privacy and Terms of Use. In D. R. Stewart (Ed.), Social Media and the Law (pp. 50-74). New York, NY: Routledge

K&L Gates. (2010). CITING FIRST AMENDMENT, COURT DENIES MOTION TO COMPEL PRODUCTION OF INFORMATION SUFFICIENT TO IDENTIFY ANONYMOUS DISCUSSION BOARD USERS. K&L Gates Electronic Discovery Law. Retrieved from https://www.ediscoverylaw.com/2010/03/citing-first-amendment-court-denies-motion-to-compel-production-of-information-sufficient-to-identify-anonymous-discussion-board-users/

Silver, D. (2013). Defamation. In D. R. Stewart (Ed.), Social Media and the Law (pp. 23-49). New York, NY: Routledge

Weckerle, A. (2013). Legal Aspects of Online Disputes and Conflicts. In Civility in the Digital Age (pp. 241-251). Indianapolis, IN: Que

WJHG. (2016). Social media: The difference between in-person and online communication. WJHG.com. Retrieved from http://www.wjhg.com/content/news/Social-media-The-difference-between-in-person-and-online-communication-386962241.html