Anna Mahanor

Dr. Daniel Panici

CMS 223

May 5, 2021

Why Data Privacy Should be in the First Amendment

Humans continue to seek new land and industrialize the globe. With each instance of invasive human habitation, the planet combats an unnatural growth with biological warfare. The most recent case is ongoing and spreads like wildfire; the environment's weapon in the global battle is COVID-19. For a brief moment, society's expansion halts and the determination to grow presents itself in a different area and the world finds itself online. The digital era, which humanity is living in, envelopes daily routines and practices with a veil of data. Individuals which once browsed through the newspaper with a coffee in hand, now sit scrolling through a screen of information. Each click and swipe happens so fast that one may forget how they found themselves on a certain website; however, every interaction online is carefully tracked, stored and used by companies for data analytics, especially during the current pandemic. So, this reveals a paradox: the many in person activities, jobs, or school programs that have been saved by moving onto digital platforms, are currently being used as a way to breach our privacy, target us, and collect more data points than ever. The pandemic created a gold mine for analytics companies and corporations, they are thriving from the mass amounts of data points available for targeted marketing. With this being said one may ask: *how is this a crisis*?

The problem, put simply, is that our privacy is in danger. Privacy, by definition, is the state or condition in which an individual is free from being observed or disturbed by other people (Oxford Languages). When we are online we do not actually have any privacy because

“whenever you use the Internet, you leave a record of the websites you visit, along with each and every thing you click. To track this information, many websites save a small piece of data—known as a **cookie**—to your web browser (*GCFGlobal.org*).” There are many different types of cookies, there are sessionary cookies, persistent cookies, tracking cookies, and third party cookies (americanbar.org). Many websites will have you agree to their terms and conditions, which will include the use of cookies on the website; yet sometimes the website will just state that cookies are necessary in order to operate. There are some individuals that are thrilled at the fact they can pick up where they left off on a website, because of sessionary cookies, and perhaps they find it tasteful that they are receiving targeted advertisements from persistent cookies, which improve their browsing experience. Still, cookies are not as refined as one may initially think. “Privacy concerns [have] become more urgent as computers—whose security is sometimes breached—amass private information in central databases that can be disseminated instantaneously over the Internet” (Lee, 184). The issue lies within the fact that our technologically driven society is advancing faster than new privacy laws can be established or refined; essentially we are vulnerable because our data is at risk. The solution? Privacy should also be included in the First Amendment.

In 1969 Supreme Court Justice Thurgood Marshall wrote on the Stanley v. Georgia case stating: “If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving [the] government the power to control men’s [or individual’s] minds” (*Privacy*). Fifty-two years later Justice Thurgood Marshall’s statement could be geared towards not the government per say, but the analytic companies that are using our data for subliminal advertisements and messaging. Currently there

is an “unilateral claiming of private human experience as free raw material for translation into behavioral data. These data are then computed and packaged as prediction products and sold into behavioral futures markets — business customers with a commercial interest in knowing what we will do now, soon, and later” (*American Bar Association*). Essentially we are given personalized advertisements and reorganized feeds based off of our data, yet both of these customized digital features potentially infringe on individuals rights to search for truth in the marketplace of ideas. According to Professor Frederick Schauer, “there are several First Amendments, each with different theoretical justifications for different circumstances. One First Amendment, according to Schauer, serves the goals of democratic governance by forbidding [the] government to suppress the political speech of its critics [which personalized feeds do through creating an echochamber that reinforces political opinions]. Another First Amendment is justified by the [aforementioned claim that one has the right to] search for truth in the ‘marketplace of ideas’” (Lee, 29-30). How are we guaranteed our First Amendment rights when our feed is selected based on predictions from our data and how can we address this? “From a privacy perspective, there are two key concepts that are at tension with the use of cookies to collect personal information: transparency and control” (*American Bar Association*). The EU’s GDPR, requires websites to present the user with knowledge that cookies are being used, but users still misunderstand what the use of cookies actually means; they do not realize that “the creation of massive online dossiers on individuals, [is unavailable to them and] is derived through the use of cookie and tracking technologies” (*American Bar Association*).

It should be noted that privacy is prevalent within the U.S. constitution and recently there was a landmark 2018 case, Carpenter v. U.S., which involves data privacy and tracking technologies. The Supreme Court ruled police must first get a warrant to access a person's

sensitive cell phone's location data (*Lawfare*). However, this ruling is based off of the fourth amendment that prohibits unreasonable searches and seizures. There have actually been several cases in which location privacy has been an issue, this can be seen in the U.S. v. Jones case, still there are few cases that document data protection rights in the United States. An exception to this is the Privacy Protection Act of 1974, which "establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies" (*The United States Department of Justice*). Still the PPA comes six years prior to when we technically began the technological or digital era; so it is necessary to refine and create new ways to protect the privacy of people. Therefore it is crucial for the "political and judicial philosophies of the judges [to take data privacy into account], and particularly their interpretation of the First Amendment, [so they can] determine the boundaries of freedom for [online] communicators" (Lee, 8). In order to protect freedom within the United States, we must regulate how corporations can use cookies, as well as our data, and incorporate data privacy into the First Amendment.

Works Cited

Haydel, Judith. *Privacy*, www.mtsu.edu/first-amendment/article/1141/privacy.

"Internet Safety: Understanding Browser Tracking." *GCFGlobal.org*, edu.gcfglobal.org/en/internetsafety/understanding-browser-tracking/1/.

Lee, William E.; Stewart, Daxton R.; Peters, Jonathan. The Law of Public Communication Taylor and Francis. Kindle Edition.

"Privacy Act of 1974 - Explained." *The Business Professor, LLC*, thebusinessprofessor.com/consumer-law/privacy-act-of-1974.

"Privacy Act of 1974." *The United States Department of Justice*, 30 Apr. 2021, www.justice.gov/opcl/privacy-act-1974.

"Summary: The Supreme Court Rules in Carpenter v. United States." *Lawfare*, 31 Oct. 2019, www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states.

"Web Cookies and Shadow Data Collection: The Legal Implications." *American Bar Association*, www.americanbar.org/groups/business_law/publications/committee_newsletters/cyberspace/2020/202005/fa_2/.