Regulating the Internet Assignment

Regulating the Internet Assignment

Nathan Ketterlinus

April 7, 2024

Towson University, COSC418-102, Steven Evans

Abstract

This paper was written to address the question in the week 9 assignment for COSC418. It is broken into two parts. The first will examine six different articles on privacy on the internet, and consider how the points they articulate fit in with the wider ethical frameworks of Deontology (specifically Kantianism) and Utilitarianism. Findings include the implication that mass data harvesting is unethical because it treats individuals as means to an end and the importance that ISPs play in keeping the internet equitable for all. The second part of the paper examines the terrorist attacks of 9/11 as a catalyst event. It looks at the immediate changes sparked by the event, such as the war on terrorism and the creation of the Department of Homeland Security, as well as considers the lasting effects that these decisions have had on the American population. The President’s Surveillance Program and Edward Snowden’s subsequent leaking of the specifics of this program are provided as a case study.

Regulating the Internet Assignment – Part 1

The structure of the first part of this paper will look at six different articles and analyze how the information in them can be applied to ethical theories. Sources range from ABC news to Stanford.

The first article to be looked at is ABC news’s “Retailers tracking shoppers’ locations in the real world”, from 2017. The article focuses on how physical retailers like Macy’s and Urban Outfitters have apps that utilize user’s “GPS, Bluetooth, WiFi, and microphone” privileges on their phones to accurately track them (ABC News, 2017, para 9). The companies justify this as a form of marketing: Macy’s is cited numerous times throughout the article giving customers personalized deals whenever the app detects them close to a store or in a competitor’s store (ABC News, 2017, para 11). While the savings these coupons provide may justify the data cost for some, the implications of every retailer app installed on a phone constantly tracking users and sending spam advertisements seems obnoxious at best, and dystopian at worst.

As it pertains to ethical theories, these advertising tactics are unethical from both a deontological and utilitarian framework.

Deontologically (specifically through Kantianism), companies advertising with location data are not acting in a way that treats people as ends, but rather a means to the company’s own ends: improving their bottom line. In addition, advertising to customers in a competitor’s store is not a universalizable maxim for the same reason that stealing is not a universalizable maxim. Through the lens of utilitarianism, these companies fail because they are jeopardizing millions of people’s PII. How often do cases of data breaches come up where people’s private data is made public? Even though current law says the personal data can be collected so long as accurate and reasonable lengths are taken to protect it, an argument can be made that any stored data is susceptible to attack (especially 0-day attacks), and thus it is unethical to risk people’s data for that reason alone.

Thomson Reuters has an article outlining various internet privacy laws and steps users can take to protect their data online. Discussed laws include the FTC act of 1914, the ECPA of 1986, the CFAA of 1986, the COPPA of 1998, the CAN-SPAM Act of 2003, the GLBA of 1999, and the FACTA of 2003 (Thomson Reuters, n.d.). The article then informs users of tips to make their web browsing safer, their cookie use more scrutinous, their IP address private, and their cloud computing more secure. The tips listed are a bit rudimentary and common knowledge for people that use computers every day: HTTPS is more secure than HTTP (Thomson Reuters, n.d.). Generally, however, the tips are relevant enough to the average person that they will benefit from at least one of the tips provided.

From a Utilitarian perspective, this article is great. Comparing two worlds where this article did or did not exist, more utility is generated from this article’s publication. It liberates the reader to take more control of their data, while simultaneously limiting the amount of insight and information (and thereby control) businesses have over their customers.

While some may argue that taking this control away from businesses generates negative utility for the businesses, the magnitude it benefits the swaths of individuals far outweighs this concern. This article is quite clear cut deontologically too. It upholds all three of Kant’s categorical imperatives, meaning its ethically sound.

The third article we will look at discusses laws in various states that are aimed at protecting the individual’s digital privacy. The article breaks these laws into two parts: one that outlines the consumer’s privacy rights and privileges they can exercise to uphold these rights, and the proper procedure data brokers and advertisers must follow to uphold the integrity of their customer’s privacy (NCSL, 2022). The article only lists laws from a select few states, including California, Nevada, Vermont, Maine, Minnesota, Nevada, Delaware, Arizona, Missouri, Connecticut, and Oregon (NCSL, 2022). Laws discussed tackle a wide array of situations, ranging from e-Reader privacy to the protection of PI by ISPs. All laws that deal with the privacy of children, such as Calif. Bus. & Prof. Code §§ 22580-22582 and Del. Code § 1204C, are much stricter and have much narrower definitions as to what constitutes acceptable use of a minor’s data, and limits targeted advertising to age appropriate material.

Again, these laws are pretty ethically sound. They are utilitarian in that they sacrifice the profits of a few companies in the interest of the privacy of millions. They are deontological because they uphold the sanctity of the individual’s privacy, treating them as an end and not jeopardizing companies using this data to treat the individual as a means to an end.

Fourthly, we will dissect a New York Times article entitled “The State of Consumer Data Privacy Laws in the US (And Why It Matters)” (Klosowski, 2021). The thesis of this article is that a general, strict federal privacy law needs to be set in place so that privacy laws are much simpler for companies to implement, and much easier for consumers to be educated on.

The article mentions a few concerns that are indicative of American sentiment on privacy as a whole, like the “privacy is dead” notion that many feel that can be alleviated by a well implemented federal privacy law (Klosowski 2022). Another important topic brought up that the author would like to see in a theoretical federal privacy law is the concept of “privacy by default” (Klosowski, 2022, para 30). This concept includes the idea of consumers opting in to let companies use their data, as opposed to the sisyphean system of opting out of data collection that is commonplace now.

Similarly to how this article expands the scale of the conversation of privacy to the federal level, this article also expands the ethical conversation of these laws to the federal level as well. When discussing previous articles, the framework was always in the context of a singular state at a time. Now, however, the conversation is shifted to examine how the patchwork of smaller-scope laws we have now combine to influence the American population as a whole, as well as companies operating on this new, larger scale. Particularly, the ethicality of a patchwork solution is called into question when considering the effort companies have to go to in order to comply, and the lengths customers have to go to in order to stay caught up on their government-protected rights. Are these laws really generating the greatest good when companies and individuals need teams of fully qualified legal experts to understand the various policies in effect everywhere?

The fifth article describes a major international ISP, Cogent, cutting all services to Russia in response to their invasion of Ukraine (Roth, 2022). The move is partially motivated by Cogent wanting to stay in compliance with the European Union following their “move to ban Russian state-backed media outlets” (Roth, 2022, para 2).

Cogent also claims that the move is intended to stop the Russian government from using Cogent’s network for “cyberattacks and propaganda” (Roth, 2022, para 6). Critics of the move, however, claim that the company is limiting Russian citizens from accessing independent news sources on the Russian-Ukrainian conflict.

Ethically, this situation is intriguing for a few reasons. First off, critics of the move are implicitly arguing that ISPs have a duty to provide internet for everyone they can, and subsequently argue that in today’s world, internet access is something close to a positive right, needing to be provided by these companies to all people. Secondly, the debate between Cogent’s reasoning for leaving Russia and critics claiming the move silences the free media is not something that has a clear right and wrong answer. Is it ethically okay for Cogent to provide a service to Russians, knowing that the government is using the product to manipulate its people in the hope that a few get accurate news? On the other hand, is it okay for Cogent to pull the plug and jeopardize the flow of information to that many people just to attempt to combat propaganda and corruption? Cogent made their decision with the facts that they had available, and now the rest of the world has to bear the consequences.

Finally, we consider an article published on Stanford’s website on the topic of net neutrality. Net Neutrality is the idea that ISPs must treat all internet traffic equally, regardless of who it comes from. For instance, Google can’t buy a “fast lane” to have their traffic route faster to customers, because it would be unfair to smaller businesses who may not be able to afford it. In effect, net neutrality allows the internet to be as free and wide-spanning and creative as it is, without fear of being dominated by only the richest companies able to afford prices analogous to extortion set by ISPs.

Ethically, net neutrality is clearly a good idea. It provides the most utility (in this case creative, cheap, and beneficial web products) for the most people, while only limiting the profits of those who would dare to violate it. Deontologically, it also treats people and small businesses as a means to an end. It gives them a fair shot to compete with bigger businesses instead of just seeing them as a way to extract more money.

After reviewing all six articles, a few summarizable ethical notes are presented. First, the conclusion can be made that when companies turn customer data into a mass collection, for-profit model, it can be argued that the person becomes seen as nothing more than their data and a company’s potential profit. This, in turn, means that the individual is seen as an end, as opposed to a means to an end, violating Kant’s categorical imperative. Therefore, one can conclude that it is unethical for companies to harvest mass amounts of user data with profit in mind. Secondly, one must consider the increasingly important role ISPs play in the modern world. As it becomes harder and harder for people to live without the internet, ISPs have the incredibly important role of ensuring equal and equitable access to the internet to all people, and the difficult task of upholding this principle and the principle of net neutrality even when it might mean turning down a better bottom line.

Regulating the Internet Assignment – Part 2

Catalyst events are events that have happened that have sparked radical changes when they happened, as well as left a lasting impact on current practices. Examples include the Constitution influencing the way the United States (and other countries) write their laws and the Chernobyl disaster impacting the way the world thinks about nuclear energy. The topic of this section of the paper, however, focuses on the terrorist attacks of 9/11, its relevance in the modern world, and how it continues to impact us today.

As a quick summary for those that do not know, the 9/11 terrorist attacks refer to Al Qaeda, a terrorist group from the middle east, hijacking four commercial airplanes and flying them into two of the world trade centers in New York City, the Pentagon in Virginia, and a field in Pennsylvania (History.com, 2023). In total, 2,996 people died in this attack, which served as a wake-up call to the United States (and to a lesser extent, the world), to tighten up their security protocols and begin waging the war on terrorism (History.com, 2023, para 22).

As mentioned above, this tragic event is relevant because it shaped how the United States as a nation approaches security. The fact that people separate the history of the country into a “pre 9/11 world” and a “post 9/11” world should be evidence enough that this event has had a lasting impact. Although I cannot speak to it personally, as I was born in 2004, I have heard just how much more difficult it is to travel by plane in the post 9/11 world. Airport security practices have gone so far that they would seem almost dystopian to anyone before the attack, but we have collectively signed the social contract that we are willing to put up with such practices in hopes to prevent such an attack from ever happening again.

Furthermore, as a testament to the impact this attack had on the United States, former president Bush used the attack to declare a war on terrorism, create the Department of Homeland Security, and begin the invasion of Iraq (History.com, 2023, para 2). In order to accomplish all of these goals, the government’s executive power was significantly expanded. The Bush Administration had “authorized spying on Americans, a new secretive military tribunal system, and begun secretly detaining men from Muslim and Arab countries” (Carlisle, 2021, para 2). Probably most infamously, however, was the launch of the President’s Surveillance Program (PSP).

PSP included the “warrantless wiretapping of communications of people thought to be connected with al-Qaeda, and the warrantless collecting and mining of Americans’ phone and internet metadata” (Carlisle, 2021, para 21). The details of this program were leaked by Edward Snowden in 2013. This chain of events, while convoluted, has irrevocably changed how the American population views and trusts the international community, as well as their own government.

This section of the paper has analyzed the terrorist attacks of 9/11 as a catalyst event. Specifically it looks at how 9/11 sparked dramatic change at the time of the event, and examined how these changes have had a lasting impact on the United States even into the present day.

References

ABC News. (2017, June 5). *Retailers tracking shoppers’ locations in the real world*. <https://abcnews.go.com/Technology/retailers-tracking-shoppers-locations-real-world/story?id=47825826>

Carlisle, M. (2021, September 11). *How 9/11 radically expanded the power of the U.S. Government*. Time. <https://time.com/6096903/september-11-legal-history/>

History.com. (2023, August 9). *September 11 attacks: Facts, background & impact*. <https://www.history.com/topics/21st-century/9-11-attacks>

Iskandar, T., Semien, L., & Vinegrad, D. (n.d.). *Net Neutrality*. Net neutrality. <https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/NetNeutrality/Articles/Proponents.html>

Klosowski, T. (2021, September 6). *The State of Consumer Data Privacy Laws in the US (and why it matters)*. The New York Times. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

NCSL. (2022, June 7). *Report state laws related to Digital Privacy*. National Conference of State Legislatures. <https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy>

Roth, E. (2022, March 5). *Internet backbone provider shuts off service in Russia*. The Verge. <https://www.theverge.com/2022/3/5/22962822/internet-backbone-provider-cogent-shuts-off-service-russia>

Thomson Reuters. (n.d.). *Internet privacy laws revealed - how your personal information is protected online*. Internet Privacy Laws Revealed - How Your Personal Information is Protected Online | Thomson Reuters. <https://legal.thomsonreuters.com/en/insights/articles/how-your-personal-information-is-protected-online>