Data Profiteering: Corporate Social Responsibility and Privacy Law Lost in Data Monetization and National Security

John B. Taschner

School of Law, The City University of New York (CUNY), New York, **USA**

ABSTRACT

Data mining and collecting is increasingly becoming a common practice, in the name of monetization of personal data, progression of national security measures, and politically fueled democratic interferences. Millions of users' data is constantly being sorted, manipulated, and sold, often without conscientious consent of the consumer. While this practice can result in greater convenience from an innocent consumer level, the vulnerabilities to national privacy and the cyberspace create dangerous territory.

The article entitled describes the triangulation of security, monetization, and politicizing in terms of data collection through three primary case studies: Cambridge Analytica and the Facebook scandal during the 2016 United States presidential election, Apple v. FBI, and Edward Snowden and the NSA surveillance activities. It explores how data harvesting and subsequent monetization is embedded in virtually every aspect of our culture and develops understanding of how corporate social responsibility calls for companies to respect and maintain transparency with consumer interests.

Current technology policies leaves open spaces for violation both internally and internationally, and why this constitutes certain offensive measures. Future data and privacy legislation, with strong consideration to the varying social contexts, resources, and current international relations. This is done under the underlying assumption that data is an irreplaceable factor in our global progression and is irrevocably embedded into our society. Over-regulation or under-regulation of big tech may lead to negative repercussions to our security or individual privacy rights.

These ideas are becoming increasingly understood by the general public and are considered worthy of concern after seeing glimpses of the depth of surveillance and information held by either the government or corporations. While there are intense emotions and opinions on the matter, my article takes an objective and well-rounded perspective to address the interlocking complexities of individual freedoms, need for international cyberspace protection, and continued profitability of data. The idea of personal data and information being manipulated and used against citizens for financial or political agendas is rightfully horrifying the public; my article therefore takes into account these concerns while suggesting further navigating the political, legal, and social process in alignment with the ever-growing power of big data.

Keywords: data profiteering, corporate social responsibility, business ethics, consumer privacy, national security, data mining

INTRODUCTION

Knowledge of the process by which personal data is monitored, tracked, and then sold countless times for corporate fiscal gain is no longer limited only to scholars: the public is slowly becoming aware of the problematic profiteering deals that previously occurred in the dark. This information that they gather includes credit card information, social security numbers, digital communication history like chat logs, text messages, and emails, health history, web search history, physical location history, and more.[1] Each of these data points are carefully tracked, monitored and sold hundreds of times to the extent that companies often know you better than you know yourself. To be considered: investigative journalists pressed into Cambridge Analytica and Facebook and found undeniable evidences proving that Facebook had utilized its massive data storage possessions to influence swing voters during the 2016 United States election and push Donald Trump to victory. This was done by an application called "thisisyourdigitallife" which featured a personality quiz in an app that recorded results and collected data from quiz takers' Facebook accounts as well as the quiz takers' friends' Facebook accounts. This data was then pushed through an algorithm that enabled psychological profiling based on Facebook interactions.[2] Progressions in data and technology are excellent tools that display the greatness and vast creativity of human minds, but recent elections have raised critical questions about the usage of such influencing data techniques and their implications for authentic democratic processes.

In effort to improve transparency and public rapport, large corporations such as Facebook now release data policies to answer key questions about privacy: "What kinds of information do we collect?"; "How do we use this information?"; "How is this information shared?"; How do we operate and transfer data as part of our global services?" and more.[3] Digital technological advancements have brought major changes, but unresolved moral and ethical issues continue to emerge.[4] Digital privacy is a developing field, that unfortunately often struggles to keep up with the rapidly quickening pace at which technology itself evolves. Several major lawsuits and scandals that have occurred in recent years have made it more imperative and prioritized for new legislation and regulation to occur for companies or organizations that harvest data for lucrative or claims of security purposes. How this necessary regulation can be done without violating the laissez-faire economic and governmental policies that are heavily favored in the United States remains difficult.

This Article will endeavor to meet this challenge by exploring how data harvesting and monetization impacts social behaviors, events, corporations, and individuals, to explain how exploitation is distinctive from influencing, to develop understanding of how corporate social responsibility relates to privacy obligations, to investigate how current technology leaves gaps for privacy rights and exploitation, and to describe how to navigate the regulation process independently or through legislation. I aim to contribute to the philosophical explanations of exploitation by discussing and providing examples of the root of these concepts, and placing special emphasis on how these have evolved throughout digital technological advancements. The Article will also engage with politics, the law, and developing public policy in accordance to protection of citizens' personal information data.

In Part II of the Article, I will describe cases that have formed the backbone for our present legislation regarding data monetization and privacy rights. In Part III, I build on the nature of these cases, discuss the obligations of corporations to practice social responsibility, and explore the legislative options to regulate businesses managing users' data to argue that there are certain moral duties that must be met by large corporations and that governing bodies must play a role in the regulation of modern data usages.

I conclude by suggesting direction for data and privacy legislation in the future, with consideration to the various social contexts we currently live in. Technology and its influence can be beneficial in using data to suggest consumer products that are appropriate for our lifestyles, but less positive in harvesting data to sway political elections. I argue that the consumerism aspect of data mining and collection is less critical than an autonomous political decision, and advocate for limitations and regulation on the types of harvested data as well as its usage. As we collectively begin to combat the deliberate

[1] Source: Aricent/frog design, primary research (2011). Graph of the "Revealed Value of Personal Data". This reveals the highest value of personal data to be your social security number/government ID at $240.00, followed by your credit card information at $150.00 and digital communication history at $59.00.

[2] See Ikhlaq ur Rehman, "Facebook-Cambridge Analytica data harvesting: What you need to know", *Library Philosophy and Practice (e-journal),* (2019). Description of the manner in which Cambridge Analytica harvested the personal data of users, as well as the repercussions of such extreme privacy violations.

[3] Facebook, *Data Policy* (April 19, 2018), https://www.facebook.com/policy.php, [https://perma.cc/4X53-ALXY]

[4] Etter, M., Fieseler, C. & Whelan, G. Sharing Economy, Sharing Responsibility? Corporate Social Responsibility in the Digital Age. *J Bus Ethics* **159,** 935-942 (2019). https://doi.org/10.1007/s10551-019-04212-w

violations of user privacy at the hands of large corporations and press more effectively for the monitoring of their actions, it is important to note the difference in social effect between data mining utilized for consumerism versus that used for political gain.

MAJOR CASES INVOLVING DATA PRIVACY AND USER DATA

In order to demonstrate the criticality of this issue and provide a basis for the suggested amendments to the current climate, I introduce several well-known cases to the discussion. These cases give consideration to the extraneous factors like national security, terrorism, and post-humous rights to privacy. Though several whistleblowers have gone public with information on technology uses that typically are kept private, one of the most notable has been the revelations made by former National Security Agency contractor Edward Snowden regarding the surveillance activities of the governments of the United States, United Kingdom, and their allies.[5] In the case *Apple v. FBI*, the conflict centered on encryption and data privacy between the government and technology companies.[6] This case was critical in the development of understanding the role of government in protecting data privacy, as well as emphasizing the role technology can play in terrorism. Lastly, I will also be referencing the Cambridge Analytica and Facebook scandal, which highlighted the extensive data mining practiced by the social media giant that was then utilized for political purposes during the 2016 United States Presidential Election.[7] Combined, these three legal cases and scandals clarify and explain the national concerns about technology, privacy and security.

A. Monitoring American Devices for "National Security"

There is a controversially fine line between what constitutes investigative journalism and espionage. According to the Cornell Law School's Legal Information Institute, espionage is defined as "the act of spying on or monitoring the activities of a government company in order to gather secret information".[8] Edward Snowden was an IT systems expert who was working for the National Security Agency (NSA) when he made the choice to become a whistleblower by sharing thousands of top-secret documents about the United States intelligence agencies' surveillance of Americans with journalists from *The Guardian*, *The New York Times*, and *The Intercept*.[9]

Since the terrorist attacks on the World Trade Center in New York, the NSA's mass surveillance had greatly expanded. Snowden provided proof to the journalists that the government was regularly tracking the calls of millions of Americans, unbeknownst to the citizens who were being spied on. These 2013 revelations startled the American population, who suddenly began to recognize the complexities of the ambiguous levels of data and privacy security they possessed.

This exposure of the government's surveillance activities shows how in the dark much of the public is when it comes to technology, data privacy, and security. Users are not offered waivers to allow the government to spy on their personal calls, texts, or emails, but still government agencies partake in these activities citing laws like the FISA Amendments Act (FAA), Executive Order 12333, and the Patriot Act. The FAA "authorizes foreign intelligence surveillance activities that have been vital to keeping the nation safe" and was used as the primary source of legal precedent for the NSA's actions that were exposed by Edward Snowden.[10] Executive Order 12333's goals included: "the United States intelligence effort shall provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense and economic policy, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill

[5] *See* Ewan MacAskill, *'They wanted me gone': Edward Snowden tells of whistleblowing, his AI fears and six years in Russia*, THE GUARDIAN (Sept. 13, 2019), https://www.theguardian.com/us-news/ng-interactive/2019/sep/13/edward-snowden-interview-whistleblowing-russia-ai-permanent-record [https://perma.cc/99LE-G3PT]

[6] *See* epic.org, '*Apple v. FBI*', EPIC.ORG ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/amicus/crypto/apple/#:~:text=An%20internal%20investigation%20has%20revealed,to%20unlock%20an%20encrypted%20iPhone.&text=EPIC%20filed%20an%20amicus%20brief%20in%20Apple%20v.,to%20protect%20consumers%20from%20crime.%22

[https://perma.cc/J29K-GCBA]

[7] *See* Iga Kozlowska, *Facebook and Data Privacy in the Age of Cambridge Analytica*, *THE HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES AT THE UNIVERSITY OF WASHINGTON*, https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/, [https://perma.cc/V5HH-GT2F]

[8] *See* Cornell Law School, *Espionage*, *LEGAL INFORMATION INSTITUTE OF CORNELL LAW SCHOOL*, *https://www.law/espionage* [https://perma.cc/3JA9-7HP9]

[9] *See* Hanna Kim, "The Resilient Foundation of Democracy: The Legal Deconstruction of the Washington Posts's Condemnation of Edward Snowden", *Indiana Law Journal*: Vol. 93: Iss. 2, Article 8 (2018), https://www.repository.law.indiana.edu/ilj/vol93/iss2/8/ [https://perma.cc/JS42-LGKU]

[10] *See The FISA Amendments Act: Q & A*, https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf [https://perma.cc/L6ZJ-LCZJ]

this goal".[11] The Patriot Act has been both the most recent and recognizable government act in terms of privacy and security, and was formed immediately following the September 11, 2001 attacks. The act broadly expanded law enforcement's rights to surveillance and investigative powers by giving sweeping search and surveillance privileges to domestic law enforcement and foreign intelligence agencies and eliminating the checks and balances system that was previously used by courts to ensure that those powers were not abused.[12] These three legislative movements gave a green light to many questionable acts of digital surveillance of citizens by the United States government bodies, citing national security, and were relatively unquestioned until Edward Snowden's exposure of the NSA.

The value of protecting the nation and its citizens in the cyberspace is so high that the United States Army has its own branch dedicated to global operations and protecting the nation against cyberspace attacks. U.S. Army Cyber Command (ARCYBER) serves to "operate and defend Army networks and deliver cyberspace effects against adversaries to defend the nation".[13] Still, there is little comprehendible transparency with the American public as to what specifically their defensive actions entail, as so much surveillance can be justified by "defending the nation".

B. Monitoring American Devices for "National Security"

While national security should be high priority, the specific regulations and policies for what this looks like has been controversial. In the case *Apple v. FBI*, national security was initially brushed off as being secondary priority to the protection of user privacy. On December 2, 2015, a married couple named Syed Rizwan Farook and Tashfeen Malik opened fire at the Inland Regional Center in San Bernardino, California, killing fourteen and injuring 22 more.[14] This act of terrorism horrified the American public, but also began a tense conversation about reasonable user privacy and data rights after a cell phone owned by the terrorists was discovered. The phone, made by Apple, could contain key evidence and provide assistance to law enforcement.

Nonetheless, a legal dispute ensued in which the FBI applied for an order that required Apple to invent a custom operating system that would disable key security iPhone features and access encrypted data. The Court then issued an order that required the creation and installation of this custom hacking tool without unlocking or otherwise changing the data on the phone. In response, Apple claimed that the order was both unlawful and unconstitutional, and argued that it would undermine the security of all Apple devices as well as setting dangerous legal precedent.[15] The company argued specifically that "[t]he All Writs Act does not provide a basis to conscript Apple to create software enabling the government to hack into iPhones" and that the Order "would violate the First Amendment and the Fifth Amendment's Due Process clause".[16]

Apple has struggled in the past in terms of user perception towards their products. There were frequent issues in terms of phone batteries dying at an accelerated rate, particularly once they passed a certain age. Users were suspicious that this was to encourage owners to purchase newer models more frequently, leading to greater profit for Apple. The company finally admitting to slowing down older iPhones because of ageing batteries in 2017, only after years of rumors.[17] When it comes to user perception, corporation hold consumers' opinions in high esteem. It would not have been a good look for the company to open

[11] Signed by President Ronald Reagan in 1981, Executive Order 12333 related to the effective conduct of United States intelligence activities and the protection of constitutional rights. *See Executive Order 12333*, NATIONAL ARCHIVES, (December 4, 1981). https://www.archives.gov/federal-register/codification/executive-order/12333.html#1.1 [https://perma.cc/M5FH-5KUC]

[12] See *Electronic Frontier Foundation*, "PATRIOT Act", (13 July 2020), https://www.eff.org/issues/patriot-act#:~:text=The%20USA%20PATRIOT%20Act%20(officially,the%20September%2011%2C%202001%20attacks. [https://perma.cc/P7ZB-SXVH]

[13] *About Us*, U.S. ARMY CYBER COMMAND, (June 2020), https://www.arcyber.army.mil/Organization/About-Army-Cyber/ [https://perma.cc/5VSD-YXAW]

[14] *Case Study: San Bernardino mass shooting*, THOMSEN REUTERS (15 July 2020), https://legal.thomsonreuters.com/en/insights/case-studies/san-bernardino [https://perma.cc/D722-C2KE]

[15] For summary, background, documents, and news on the case, see epic.org, *Apple v. FBI: Concerning an Order Requiring Apple to Create Custom Software to Assist the FBI in Hacking a Seized iPhone*, ELECTRONIC PRIVACY INFORMATION CENTER (2020), https://epic.org/amicus/crypto/apple/ [https://perma.cc/FW4F-6AHN].

[16] For more detail, see "APPLE INC'S MOTION TO VACATE ORDER COMPELLING APPLE INC. TO ASSIST AGENTS IN SEARCH, AND OPPOSITION TO GOVERNMENT'S MOTION TO COMPEL ASSISTANCE" in response to "IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE SEIZED DURING THE EXECUTION OF A SEARCH WARRANT ON A BLACK LEXUS IS300, CALIFORNIA LICENSE PLATE 35KGD203", https://epic.org/amicus/crypto/apple/In-re-Apple-Motion-to-Vacate.pdf [https://perma.cc/XYM5-6HJ5]

[17] See Samuel Gibbs, "Apple admits slowing older iPhones because of ageing batteries," *The Guardian*, (December 21, 2017), https://www.theguardian.com/technology/2017/dec/21/apple-admits-slowing-older-iphones-because-of-flagging-batteries [https://perma.cc/Z4SV-ZUF5]

up a phone, regardless of it being owned by a terrorist, because it would inevitably lead to the conclusion that Apple can open and unlock any iPhone without express user consent. Fortunately for Apple, the FBI was ultimately able to unlock the iPhone in question without their assistance and withdrew their request. Still, the *Apple v. FBI* case became significant because of its highlighting of the issue of constitutional rights to privacy against government and corporations.

C. Political Exploitation of User Data

The final instance of user privacy cases to be discussed is the 2016 Facebook and Cambridge Analytica scandal in which a former employee of Cambridge Analytica that worked for Donald Trump's victorious presidential campaign alleged that the company had used Facebook in order to bombard specifically chosen individuals with misinformation in hopes of swaying their political views.[18]

These accusations in turn led to a Senate hearing in which Facebook's CEO Mark Zuckerberg was called in to testify. During proceedings, he was questioned on the security and privacy of Facebook, citing the fact that "a quiz app used by approximately 300,000 people led to information about 87 million Facebook users being obtained by the company Cambridge Analytica" and asking "why didn't Facebook notify 87 million users that their personally identifiable information had been taken, and it was being also used – why were they not informed – for unauthorized political purposes?"[19] In an article by the *New York Times* covering the subsequent congressional hearing, senators were quoted as having said "they weren't sure if they could trust a company that has repeatedly violated its privacy promises."[20]

Many believed that the scandal would lead to increased regulation of Facebook and the tech industry. Instead, our global pandemic and current campaign strategies are hard evidence that our politicians and tech giants have merged to create a joint venture in which tech has more power, more money, and more ability to influence than any government.

Whenever we post a status on Facebook pages or send an innocuous 140-character tweet, this data travels somewhere. Theodore F. Claypool is Chair of the American Bar Association's Cyberspace Committee in the Business Law Section, and said in a magazine published by the American Bar Association, "every bit of information we disclose is another databite to be mined and measured, sorted and sold."[21] Everything from our children's photos to GPS location data is then owned by major tech figures. Once it is online, it is neither yours nor completely erasable. There is no such thing as an innocent or inconsequential Internet search, web surfing or browsing anymore. Every search and posting down to the individual keystrokes are tracked, sorted, scored, and saved by identifiable markers such as names, search history, birthdates, friend groups, areas of interest internet or video chat patterns, and more are captured and used in various ways by unknown people, agencies, or collection systems without any awareness of the person initiating the search. Likewise, the advancing technologies allow for various actors, agencies, or nation states to penetrate networks, systems, information baskets, health records, and every conceiving record on the plant. The vast and quickly growing collection of information and data, and exploitation of the information, data and access is astonishing and unprecedented.

For companies that have transformed into global technological power players, they enjoy certain amounts of power that are unattainable even by the strongest governments. Cybersecurity and the rapidly expanding role of major tech in the world are now arguably some of the largest and most important topics facing modern society. Professor Jeffrey Vagle of Stanford Law School writes "our institutions have largely failed to address these technologies' cybersecurity risks. And that is in large part because they have failed to address – and have even exacerbated – the moral hazard inherent in making and selling connected technologies", explaining the complicated moral and ethical issues that are often swept under the rug in conversations on the technologies that are heavily relied upon for digital connection.[22]

[18] See Tracey Lien, "A data mining company allegedly used Facebook to distort users' reality," *Los Angeles Times*, (March 20, 2018), https://www.latimes.com/business/technology/la-fi-tn-facebook-information-dominance-20180320-story.html [https://perma.cc/MU2D-2VSP]

[19] See Transcript courtesy of Bloomberg Government, "Transcript of Mark Zuckergberg's Senate hearing," *The Washington Post*, (April 20, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/ [https://perma.cc/E4Y6-VPWA]

[20] See The New York Times, "Mark Zuckerberg Testimony: Senators Question Facebook's Commitment to Privacy," *The New York Times,* (April 10, 2018), https://www.nytimes.com/2018/04/10/us/politics/mark-zuckerberg-testimony.html?auth=login-email&login=email [https://perma.cc/UE4D-PHW5]

[21] See Theodore F. Claypoole, "Privacy and Social Media," *American Bar Association*, (January 23, 2014), https://www.americanbar.org/groups/business_law/publications/blt/2014/01/03a_claypoole/ [https://perma.cc/LC95-LF2X]

[22] Jeffrey Vagle, *Cybersecurity and Moral Hazard*, STANFORD LAW REVIEW, (April 6, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3055231

[https://perma.cc/B69F-PE6R]

Political and Business use of Data and Corporate Social Responsibility

It has become part of everyday conversation to discuss how advertisements on our websites are becoming increasingly trafficked with "exactly what I was looking for!" However, what is often brushed off as mere coincidence is in fact a part of a much larger and darker narrative than most realize. Computers, phones, and the rapid advancements of technology have taken off so quickly that the public can scarcely keep up. These changes pose critical questions for our society and pace of progression: are these technological developments making the world a better and safer place? The former CEO of Google has said "there's no question that Huawei has engaged in some [data] practices that are not acceptable in national security." [23] There are certainly convenience benefits, but the reality of cybersecurity and the imminent breaches of data are far more dangerous than the average user realizes. The realities of cybersecurity and the drive for profits in the age of data value demands higher standards for companies engaging in these profitability schemes in order to protect consumers and their data footprint.

It has been estimated that social media users now represent 49% of the global population.[24] Without an institution in place to address cybersecurity risks, we put ourselves in great danger. The Internet, and particularly social media sites, are notorious for the mining of user data. Some of this data is used for advertising purposes, but in the last few years a much more sinister narrative has emerged in which data bytes are sold away to be utilized for political and financial gains.

In the midst of Mark Zuckerberg and Facebook's Senate hearing, the visual of a tech CEO sitting and facing a room full of our nation's legislative leaders, the American people at last began to realize that cybersecurity and the corporate usage of their data was becoming a major social issue.

A. Monetization of User Data

Once an Internet user searches a website for a certain item, the company is able to monitor and track that data. For companies like Visa, AT&T, or Facebook, this is a goldmine. The newly acquired information tells the company what the user searches for, purchases, the frequency at which they purchase, and more.

The attention and efforts that companies spend on tracking you has several different results. Firstly, they are able to recognize the types of products that you are already interested in, so they can find others similar to it that may appeal to you. Secondly, they can sell your data to other companies to continue the profit train. What is more comfortably called "advertising" could more accurately be described as "the process by which companies engage in study and selling of your data in order to make profits." Ultimately, many of the commonly browsed websites are simply data-selling companies. Once the extent of the issue is understood, then it becomes clear that these major technology players must require government restrictions in order to protect the average users' right to Internet privacy.

Big Data Value Chains are a relatively new creation that have grown with the emergence of Big Data in order to "face new data-related challenges such as high volume, velocity, and variety", and are a set of ordered steps that is mainly built for moving from data generation towards knowledge creation.[25] These types of advancements have led to data monetization, which is simply another way of describing the process of creating wealth from data. The specific channels by which this is done differ by company, but the end goal – profiting from data bytes – is universal. Data is no longer a mere passive entity, but rather an active asset to be used by corporations.[26]

The public enjoys certain freedoms, rights, and privileges in much of their everyday life, but many users do not enjoy full protections in the cyberspace. In a publication by MIT Sloan Management Review, two primary paths to data monetization are discussed. The first path is internal and focuses on the leveraging of data in order to improve company operations, productivity, products and services, while also enabling and ongoing personalized customer dialogues; the alternative path is external and involves creating new streams of revenue by making data available

[23] See Ryan Browne, "Former Google CEO Eric Schmidt says there is 'no question' Huawei routed data to Beijing", *CNBC*, (June 18, 2020), https://www.cnbc.com/2020/06/18/ex-google-ceo-eric-schmidt-no-question-huawei-routed-data-to-china.html?fbclid=IwAR1Hh06zuec_jqOLbLO2nchkCIi8Dp8eKUmgl4DZUvway29vN-hHFWZXzVI [https://perma.cc/L7LY-EMFS]

[24] See J. Clement, "Number of social network users worldwide from 2017-2015 (in billions)", *Statista.com*, (July 15, 2020), https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ [https://perma.cc/7HS4-JA52]

[25] *See* Abou Zakaria Faroukhi, Imane El Alaoui, Youssef Gahi & Aouatif Amine, "Big data monetization throughout Big Data Value Chain: a comprehensive review", *Journal of Big Data*, Vol. 7 Article 3, (January 8, 2020), https://link.springer.com/article/10.1186/s40537-019-0281-5 [

[26] *See* Payam Hanafizadeh and Mohammad Reza Harati Nik, "Configuration of Data Monetization: A Review of Literature with Thematic Analysis", *Global Journal of Flexible Systems Management*, Vol. 21, 17-34, (December 6, 2019), https://link.springer.com/article/10.1007/s40171-019-00228-3#citeas [https://perma.cc/GA2C-6NQ5]

to both customers and partners.[27] The two are not mutually exclusive, and some companies are able to effectively utilize aspects of both pathways in order to maximize their data monetization practices and eventual profiteering.

The capacity of data possessed by companies is shocking. Donald Trump and Cambridge Analytica's campaigns were so successful in 2016 because of how much data they had access to, but even in the aftermath of the scandal the specifics are unsettling. In tracking how much data Facebook had on one user, it was discovered that they had more than 2500 contacts and phone numbers, 1500 Messenger conversations, 10500 total friendships, 70 IP addresses, 140 videos, more than 250 photos, and 50 Advertisers had the user's contact information.[28]

As uncomfortable as it is to realize that companies have such extensive troves of data, the reality is that it is already happening. Each byte of data has a different value, with a range of prices at which it can be sold. According to a study done, the most valuable types of data are social security numbers or government ID, credit card information, digital communication history (which includes chat logs, text messages, and emails), web search history, physical location history from your phone or car CPS records, web browsing history, and health history.[29] The financial prospects that can come about as part of selling data make the practice incredibly appealing to corporations and is becoming an expected part of society.

B. Legal Implications of Data Monetization

Unfortunately, many Internet users are unfamiliar with the advancements of data profits and monetization. Since the progression of technology has occurred at such a rapid rate, it has been difficult to know what legal rights and protections exist for users in the cyberspace. Far too many people are simply signing away their rights to privacy without being fully aware of the implications. For those that do recognize the maliciousness that can come about as a result of third-party data access, they still may not be able to get their data back. This was the case for David Carroll, a professor of media design at The New School, who embarked on a quest to retrieve his data from Cambridge Analytica. Legal precedent demonstrated that British data protection laws allow people to request data on them that has been processed in the United Kingdom. Despite Carroll being an American, he was still entitled to this information because Cambridge Analytica was based in London.[30]

The hope was that this experience would in turn cause greater global change for all persons in regard to protection and reasonable expectation of privacy within cyberspace. Unfortunately, this was not the case. Former United States President Barack Obama once said "Change will not come if we wait for some other person or some other time. We are the ones we've been waiting for. We are the change that we seek."[31] While some legal rights do exist within the United States in terms of privacy, many of the guiding legislations were created in a world before the Internet could ever be fathomed.

One of the most commonly cited legal foundations is the Fourth Amendment of the United States Constitution. Originally created as a way to prevent citizens from being forced to house soldiers during the war, the vagueness of the wording has allowed it to be interpreted as rights to privacy online in the 21st century: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[32]

This amendment now provides the baseline for privacy law and regulations of the cyberspace, but still more are needed. In *Social Media, Ethics and the Privacy Paradox*, authors Barrett-Maitland and Lynch state "the right to control access to facts or personal information in our view is a natural, inalienable right and everyone should have control over who see their personal information and how it is disseminated"[33]. In order to meet the inalienable rights

[27] *See* Suketu Gandhi, Bharath Thota, Renata Kuchembuck, and Joshua Swartz, "Demystifying Data Monetization: Companies have figured out that data can be used in day-to-day operations to reduce costs and grow revenue," *MIT Sloan Management Review*, (November 27, 2018), https://sloanreview.mit.edu/article/demystifying-data-monetization/ [https://perma.cc/N7WZ-Q8ZF]

[28] *See* Cellan-Jones, Rory. Twitter Post. (March 26, 2018), 9:16am, https://twitter.com/ruskin147/status/978304582316150784 [https://perma.cc/Q54U-2S2M]

[29] *See* More with Mobile, "Prices and Value of Consumer Data", (June 19, 2013), https://www.more-with-mobile.com/2013/06/prices-and-value-of-consumer-data.html [https://perma.cc/4YB5-UE22]

[30] *See* Issie Lapowsky, "One Man's Obsessive Fight to Reclaim His Cambridge Analytica Data", *Wired*, (January 25, 2019), https://www.wired.com/story/one-mans-obsessive-fight-to-reclaim-his-cambridge-analytica-data/ [https://perma.cc/92ZL-DC3W]

[31] *See* Barack Obama, "Barack Obama's Feb. 5 Speech", *The New York Times*, (February 5, 2008), https://www.nytimes.com/2008/02/05/us/politics/05text-obama.html [https://perma.cc/23Q2-E4JQ]

[32] *See* U.S. Constitution, Amendment 4, https://constitutioncenter.org/interactive-constitution/amendment/amendment-iv, [https://perma.cc/UAC6-PGN3].

[33] *See* Nadine Barrett-Maitland and Jenice Lynch, "Social Media, Ethics and the Privacy Paradox", *Intechopen*, (February 5, 2020),

of people as technology advances, further specific laws are a necessity.

With technology being so thoroughly embedded in virtually every industry, it sounds eerily familiar to a statement Sacha Baron Cohen made in 2019. In a Washington Post article, he challenges technological CEOs' position in America: "this is ideological imperialism -- six unelected individuals in Silicon Valley imposing their vision on the rest of the world, unaccountable to any government and acting like they're above the reach of law".[34] The six unelected individuals in Silicon Valley he speaks of are referencing the six CEOs of technology giants: Mark Zuckerberg of Facebook, Sundar Pichai of Google, Larry Page and Sergey Brin of Alphabet Inc. and Google, Susan Wojcicki of YouTube, and Jack Dorsey of Twitter. Several of these tech titans have been subject to vicious public criticism in the last few years over the inappropriate power and authority they possess simply by controlling the media narratives and massive amounts of wealth.

When Mark Zuckerberg was called in front of the Senate after the Cambridge Analytica and Facebook scandals, this was a large step forward in curbing the perceived flow of untapped power held by tech titans. Now, just a few years later, he appeared again before the Senate as part of a larger virtual hearing with several other technological leaders. With the status quo radicalization of tech marketing, advertising and politics, the perception may be altered somewhat by the upcoming antitrust hearings involving the tech, advertising, and marketing giants of well-known companies. The 15-member House Judiciary Antitrust Subcommittee will ask questions of Amazon's Jeff Bezos, Apple's Tim Cook, and Facebook's Mark Zuckerberg, and Google's Sundar Pichai. Mark Zuckerberg has testified in a Senate hearing before, but this will be the first time all four of these tech giants come together to discuss their companies' practices within the digital marketplace. Casey Newton writes for *The Verge* on what is at stake for Apple, Amazon, Facebook, and Google in this historic hearing that will take place virtually due to the COVID-19 pandemic as part of Congress' 13-month investigation on competition and digital marketplaces, and notes that "while Amazon, Apple, Facebook, and Google share some broad characteristics, they are also very different companies".[35] They all are well-known companies that possess troves of user data, but in distinctively differing ways. Nonetheless, the hearing will put one more nail in the coffin towards the relatively unmonitored relationship between politics and tech.

Already there is significant disdain for several of these companies, as they are typically built or run by billionaires off of unfair and unequal business practices. In an opinion piece by Roger McNamee for Wired, he writes "over the past 20 years, the rich got much richer, while half of the country struggled with static incomes. Nowhere is this lawlessness more rampant today than among large tech companies, who've used their power to crush competitors, suppliers, business partners, and even customers."[36] This long-standing reign of power built upon a platform of technology may be ending soon though: "the hearing can increase awareness of harmful business practices."[37]Still, others remain skeptical and believe that "the hearing is unlikely to address core antitrust issues or bring new information to the table."[38]

C. National Security Risks and Benefits

There is currently unique and much-needed space in our current national framework to provide the weapons to effectively carry out cyber offense and defense on a national and international level. The Department of Homeland Security is the United States' primary source of action in counterterrorism, cybersecurity, aviation security, border security, port security, maritime security, administration and enforcement of our immigration laws, protection of our national leaders, protection of critical infrastructure, cybersecurity, detection of and protection against chemical, biological and nuclear threats to the

https://www.intechopen.com/online-first/social-media-ethics-and-the-privacy-paradox [https://perma.cc/5DFY-NEMF]

[34] *See* Sacha Baron Cohen, "The 'Silicon Six' spread propaganda. It's time to regulate social media sites", *The Washington Post*, November 25, 2019, http://www.washingtonpost.com/outlook/2019/11/25/silicon-six-spread-propaganda-its-time-regulate-social-media-sites/ [https://perma.cc/ZZY6-YGJ6]

[35] *See* Casey Newton, "The tech antitrust hearing is shaping up to be one for the ages", *The Verge*, July 24, 2020, https://www.theverge.com/2020/7/24/21335735/tech-antitrust-hearing-apple-amazon-facebook-google-preview [https://perma.cc/ZEJ5-Z2KR].

[36] *See* Roger McNamee, "A Primer to Big Tech's Antitrust Hearing: They're (Almost) All Guilty", *Wired*, https://www.wired.com/story/opinion-a-primer-to-big-techs-antitrust-hearing-theyre-almost-all-guilty/, [https://perma.cc/H7CA-LT3E] His subheading "Apple aside, anticompetitive practices by Amazon, Facebook, and Google have corroded democracy and sabotaged the nation's pandemic response" sums up the displeased public response to big technology's actions.

[37] *See* McNamee, "A Primer to Big Tech's Antitrust Hearing: They're (Almost) All Guilty".

[38] *See* Nandita Bose and Diane Bartz, "Big Tech CEOs ready defenses for U.S. Congress hearing into their growing power", *Reuters*, July 23, 2020, https://www.reuters.com/article/us-usa-tech-congress-idUSKCN24O16K [https://perma.cc/43MG-HDPR]

homeland, and response to disasters.[39] The cybersecurity sector is of great importance to our national security, as attacks against the country are more plausible as technology develops around the world. Both the cyberspace and underlying infrastructure are at risk of dangers from physical and cyber threats. These vulnerabilities can be exploited by other nation-states or actors to steal information, money, and more. The Center for Strategic and International Studies tracks these incidents, and the following have occurred in only the last few months: Canada, the UK, and the U.S. announced that hackers associated with Russian intelligence had tried to steal information related to the COVID-19 vaccine development (July 2020), North Korean state hackers sent COVID-19-themed phishing emails to more than 5 million businesses and individuals in Singapore, Japan, the U.S., South Korea, India, and the UK in an attempt to steal personal and financial data (June 2020), cyber criminals managed to steal $10 million from Norway's state investment fund in a business email compromise scam that tricked an employee into transferring money into a hacker-controlled account (May 2020).[40]

These recent and international attacks demonstrate the severity of the situation. The Department of Homeland Security has said "our daily life, economic vitality, and national security depend on a safe, stable, and resilient cyberspace".[41] Due to the extensive potential losses that could occur as a result of a breach in cybersecurity, several federal government bodies have taken steps forward to practice surveillance in an attempt to mitigate the threats against the country. Oftentimes this surveillance is done through social media networks, as companies like Facebook and Google possess the most extensive troves of data in the world. However, this is often carried out without explicit notification to the citizen. This has led to conflict in the past, as seen by the Edward Snowden's exposure of the NSA's surveillance and the subsequent public fallout. Data observation and mining is a critical resource that is used at the national level to protect ourselves by being on both the offensive and defensive. It is so thoroughly embedded in the way our national security functions that it would be naive to believe that data mining on the corporate level can simply cease to exist through legislation.

Data is an extremely valuable asset to the nation, as it can open doors to enhanced security, offensive movements, or even political election interference. As such, both corporations and the government continue to collect, mine, and use that data for their own advances. Before their company's 2016 scandal, Cambridge Analytica had boasted that it had 4,000-5,000 data points on each voter in the United States.[42] This creates a complexity between data mining and politics insofar that it becomes clear that our political campaigns and systems rely irreplaceably on data. Moreso, the data is already available. Each day, Facebook, Google, Twitter, and other Internet platforms gather millions more bytes of data as users log on and create new content. What is already available on servers is so substantial that it is possible to find one's education, date of birth, religious position, sports played, hobbies, political leanings, and more. Any information that a person, corporation, or nation-state would be interested, can be bought for a price.

D. Moral Obligations of Corporations and Data Monetization

Since the legal field has already begun to recognize the need for imminent change in policy and procedure in the understanding of cybersecurity and data, the business sector ought to follow in its footsteps to address the imminent moral implications of their actions. In *Cybersecurity and Moral Hazard*, Jeffrey Vagle said "Because the rapid advances in connected technologies continue to yield economic benefits to technology manufacturers, our political, educational, and legal institutions are geared toward the continuation of these advances at the cost of greater security risk, borne mainly by the users of these technologies."[43] Without making change, security risks will only increase. Discussion has already taken place on what to do from a legislative standpoint, but it would be incorrect to have a complete resolution of the issue without giving note to the undeniable moral implications of data monetization.

If user privacy is not a top priority for companies, then their first line of customer advocacy in terms of cybersecurity is already down. There are certain moral obligations that people and companies must meet and

[39] *See* "Secretary of Homeland Security", *Department of Homeland Security*, (July 5, 2019), https://www.dhs.gov/secretary#:~:text=Under%20the%20Secretary's%20leadership%2C%20DHS,critical%20infrastructure%2C%20cybersecurity%2C%20detection%20of

[https://perma.cc/S6DJ-RFQN]

[40] *See* Center for Strategic and International Studies, "*Significant Cyber Incidents*", (August 7, 2020), https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents [https://perma.cc/KJ37-EUSR]

[41] *See* Department of Homeland Security, "*Cybersecurity*", (March 17, 2020), https://www.dhs.gov/topic/cybersecurity [https://perma.cc/57NK-NHDD]

[42] *See* BBC News, *"Cambridge Analytica parent firm SCL Elections fined over data refusal"*, (January 10, 2019), https://www.bbc.com/news/technology-46822439 [https://perma.cc/A3HX-W559]

[43] Vagle, "Cybersecurity and Moral Hazard".

protecting those who are susceptible must be valued. However, in today's culture, fiscal success does not always align with moral excellence. Dr. Martin Luther King, Jr. once said "there comes a time when one must take a position that is neither safe nor political nor popular, but he must take it because his conscience tells him it is right." It can be challenging to do the "right" thing in a climate where everyone else is doing the "wrong" thing and reaping financial reward. However, in order to build a lasting, loyal relations with employees and customers alike and fulfill humanitarian obligations, companies must continue to pursue further commitment to privacy. Some sites already do this, but their informing of users that their data may be tracked and monitored is often written in language that is difficult to understand or embedded in numerous paragraphs. This type of skirting action does little to inform or educate users, as most do not stop to read 500 words on a pop-up ad when they can simply click a box saying "agree" to access the content.

This comes through more transparency about what they do with their data points – making this information publicly known. Regardless of the dubious morality of the thought of using trusting users' data, it becomes much more suspicious when companies attempt to hide or cover up their actions. Although the cyberspace still has many grey areas when it comes to legal right and wrong, it is generally accepted that people should have a right to know where their own data travels to. Part of the reason why the Cambridge Analytica and Facebook hack was so shocking was because users who did reach out and try to get their data back were unable to. By raising the standards that the public has for major technological platforms, both individuals and the data information associated with them will be safer and better-protected.

A company's success is inherently tied to their connection and treatment of their workers. If they fail to treat workers fairly, then it can come back with negative repercussions for the company. Now more than ever, workers are standing up for themselves and the "right" thing to do in order to make a more positive environment. An example of this is Facebook, whose employees recently staged a virtual walkout over CEO Mark Zuckerberg's decision to leave up the Facebook version of a tweet sent by President Trump where he seemingly encouraged police to shoot rioters.[44] When Zuckerberg decided to veto the pleas of his employees and refused to shut down Trump's rampage, he made a loud statement that revealed the motives and values that his company holds. Employees who are representatives of the general public are demanding corporate social responsibility, but those who benefit from the company (like Zuckerberg) say no. Twitter's response to Trump's tweet was to hide the message behind a warning. While freedom of speech is guaranteed in the Constitution, limitations on these freedoms (particularly when it comes to violence) are also real. These types of companies have genuine moral responsibilities to care for the wellbeing of their employees and users, which ought to include intervening when necessary.

The complexities of morality and humanitarian obligations in cyberspace are underscored by the corporate social responsibility that major technology companies ought to be held to. With the vast levels of resources that they have access to and control, they have certain obligations to give back and continue to strive to make the world a better place for everyone. At bare minimum, this includes preserving the rights to privacy by users and improving transparency in their own data monetization processes. To successfully further the wellbeing of the global population will take more than simply adhering to procedure. A famous quote by Albert Einstein says, "insanity is doing the same thing, over and over again, but expecting different results". A more closely connected and convenience-driven global society has occurred through digital technology; but a safer and better world can only exist if we change the existing infrastructure, recognize cybersecurity and data as a social issue, and move forward with integrity and transparency in the age of data value.

E. Corporate Social Responsibility in Action

When companies act in a way that is morally upright and correct, it tends to attract consumers and build brand loyalty. The practice of Corporate Social Responsibility has revealed that "the company's CSR commitment induces greater satisfaction with and trust in the company and its services, which then ultimately encourages consumers to remain loyal."[45] Beyond building legitimate and long-term consumer support, this study demonstrates that there are also further financial benefits to be gained. Admittedly, this type of financial gain may take longer than the quick-fix data monetization practices, but in the long run does have its own set of respective benefits.

Corporate Social Responsibility (CSR) will be hereon understood as "an evolving concept that reflects various views and approaches regarding corporate relationships

[44] *See* Alex Hern and Julia Carrie Wong, "Facebook employees hold virtual walkout over Mark Zuckerberg's refusal to act against Trump", *The Guardian*, (June 1, 2020), https://www.theguardian.com/technology/2020/jun/01/facebook-workers-rebel-mark-zuckerberg-donald-trump [https://perma.cc/SX6V-4CQV]

[45] *See* Eunil Park, Ki Joon Kim, Sang Jib Kwon, "Corporate social responsibility as a determinant of consumer loyalty: An examination of ethical standard, satisfaction, and trust", *Journal of Business Research*, Vol. 76, 8-13, (July 2017), https://www.sciencedirect.com/science/article/abs/pii/S0148296317300784 [https://perma.cc/Q854-JHZP]

with broader society."[46] It is not a revolutionary idea, as most companies have long practiced some form of corporate social responsibility with the goal of contributing towards the wellbeing of the communities and society on which they both depend and affect.[47] Still, the execution of CSR has evolved over time, and today many scholars are advocating that CSR must shift from a discretionary or voluntary activity to an immediate and integrated response by acknowledging the major role and impact of business.[48]

When companies' CSR strategies are effective, it often results in a larger and more loyal consumer base. While companies are certain to get short-term gain from the monetization of data, users are becoming increasingly aware of this practice and are still not in full support of this. Rather than violating privacy rights and maintaining a lack of transparency, the long-term benefits of creating and nurturing a loyal customer following should be taken into consideration by major tech.

In order for a company to be sustainable, it must have clear benefits to the public and be relevant to the political and social climate of the time. Some would argue that there is not always a place for ethics within the business field and suggest that perhaps discussion on ethical behavior ought to be held outside of discussions on the practices of data privacy by large corporations. Professor and former journalist Sarah Oates states, "scholarly discussions should shift away from questions of ethics or actions (or lack thereof) on the part of social media companies to a frank focus on the security risk posed to democracy by social media"[49].

Our world is far past questioning the behavior of social media companies, their behaviors and shocking repercussions are constantly splashed across headlines. This momentum must not stop. Without a "policing" of these technology giants, the ethics and future of the domestic and international space is called into question.

F. Social Media and CSR

The first amendment has historically been the foundation for freedoms of speech and the press: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances". [50] In terms of social media platforms in the 21st century, this amendment is still typically cited as the base for allowing persons to express their political opinions, regardless of how unpleasant they may be to others. The United States is currently experiencing a highly polarized political climate, and this type of partisan split has not been seen at this magnitude before. Social media provides a platform for people to share their opinions, including the nation's President.

Donald Trump's presence on social media, particularly on Twitter, has been a defining characteristic of his presidency. It is not uncommon for political or national figures to use social media as an alternative way of communicating with large portions of the population in an instantaneous manner. In the past, it has still been an alternative option to the more formal speeches and press conferences. Trump still holds press conferences and gives speeches, as seen in his July 4th Mount Rushmore speech and daily coronavirus briefings from the beginning of the pandemic, but a president has never relied as heavily as he does on social media for primary sources of communication.

Although he does have a presence on several platforms, Twitter is his most prolific. In June, he broke a record for the most tweets and retweets made in a single day than at any other point in his presidency: 200, which broke his previous record of 142, sent during his Senate impeachment trial.[51] He has the same authority to exercise his First Amendment rights as any other American citizen, which he uses vigorously on Twitter. As a platform, Twitter is host to global dialogue ranging from

[46] *See* Anne Elizabeth Fordham and Guy M. Robinson, "Mapping meanings of corporate social responsibility – an Australian case", *International Journal of Corporate Social Responsibility*, Vol. 3, Article 14, (September 18, 2018), https://jcsr.springeropen.com/articles/10.1186/s40991-018-0036-1 [https://perma.cc/JXA4-SLZE]

[47] *See* V. Kasturi Rangan, Lisa Chase and Sohel Karim, "The Truth About CSR", *Harvard Business Review*, January – February 2015, https://hbr.org/2015/01/the-truth-about-csr [https://perma.cc/MJ5T-D4K8]

[48] *See* Myria W. Allen and Christopher A. Craig, "Rethinking corporate social responsibility in the age of climate change: a communication perspective", *International Journal of Corporate Social Responsibility*, Vol. 1, Article 1, (July 5, 2016), https://jcsr.springeropen.com/articles/10.1186/s40991-016-0002-8 [

[49] *See* Sarah Oates, "The easy weaponization of social media: why profit has trumped security for U.S. companies", *Digital War, (May 11, 2020), 1-6.* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7212244/ [https://perma.cc/RLE4-LLW9]

[50] *See* U.S. Constitution, First Amendment, https://constitution.congress.gov/constitution/amendment-1/#:~:text=Congress%20shall%20make%20no%20law,for%20a%20redress%20of%20grievances. [https://perma.cc/U95M-DHCE].

[51] *See* Connor Perrett, "Trump broke his all-time tweeting record amid national protests, sending more tweets in a single day than he did during his impeachment trial", *Insider*, https://www.insider.com/trump-breaks-record-most-tweets-in-a-single-day-2020-6 [https://perma.cc/4V6G-KSXN]

entertainment and Hollywood gossip to international politics and policy. Still, some have argued that "Twitter privileges discourse that is simple, impulsive, and uncivil".[52] In the civil unrest that has swept the nation in the last few months from the Black Lives Matter movement, from peaceful protests to looting, Trump has been very active on Twitter. The First Amendment does guarantee freedom of expression, but there are still certain policies that social media platforms hold. Twitter at last made a stand against Trump's expressiveness by hiding some of his tweets, under the description that the tweet "when the looting starts, the shooting starts" had glorified violence.[53]

This type of policing of political expression should commendation as a live practice of corporate social responsibility. While freedom of expression as guaranteed in the United States Constitution is a critical freedom of the American democracy, it should not protect blatant encouragement of violence or harm against others. Twitter, Facebook, Reddit, and other social media platforms can all do their part in fact-checking, studying, and verifying that the information that appears on their platforms will make the world a better and safer place, rather than a gathering place for the distribution of faulty and harmful opinions that can have real-world manifestations.

While Big Tech can and should be putting in effort to monitor their sites and ensure that the safety of their users is placed in high esteem, the government ought to also be playing a role in this. Similarly to our federal government system of checks and balances, so also should major tech companies and the federal government engage in relationship with one another to ensure that one does not have excessive amounts of either freedom or oppression. The way that this can be done does not require a complete overhaul and rewrite of all legislation, but rather the reforming of precedent and if necessary, the partial creation of policy that is unique to the fulfillment of needs in a technologically driven 21st century.

Future Direction for Data and Privacy Legislation

In determining where we go from here, it is critical that consideration must be given to the various social contexts. Both technology and its influence are modern developments that have created undeniable advancements across the globe, but also possess dangerous underlying and largely not understood capacities to impose their own narratives in democratic elections.

The United States currently has several organizations in place fighting global cyber threats within the Department of Homeland Security such as the National Cybersecurity and Communications. Protecting cyberspace must be a feat supported on all fronts, including privately: "the cyber realm is increasingly vital to national security, but much of cybersecurity is provided privately. Private firms provide a range of roles, from purely defensive operations to more controversial ones, such as active-cyber defense (ACD) and 'hacking back'…the reliance on private firms raises the ethical question of to what extent the private sector should be involved in providing security services".[54]

Without further involvement from all fronts, cyberspace attacks pose a unique and highly dangerous threat to our democracy. The United States is one of the longest-standing democracies in history, but the involvement of the Internet in the 2016 elections shows that the Internet can and does have very real implications. After the conclusion of one of the biggest investigations of any president in United States history, it became clear that Russian technology had indeed interfered with one of the most prominent symbols of western democracy: an election: "in recent times, actors have engaged in acts of information warfare ranging from attempts to compromising voting systems, to spreading false propaganda and even direct attacks on public infrastructure via information systems".[55] For all the objective goodness and benefits that the existence of social media provides, there is also an extremely dark and dangerous side. In *Political Warfare in the Digital Age: Cyber*

[52] *See* Brian L. Ott, "The age of Twitter: Donald J. Trump and the politics of debasement", *Critical Studies in Media Communication*, 34(1): 59-68, (January 2017), https://www.researchgate.net/publication/311892973_The_age_of_Twitter_Donald_J_Trump_and_the_politics_of_debasement [https://perma.cc/T4CX-43C6]

[53] *See* Alex Hern, "Twitter hides Donald Trump tweet for 'glorifying violence'", *The Guardian*, (May 29, 2020), https://www.theguardian.com/technology/2020/may/29/twitter-hides-donald-trump-tweet-glorifying-violence [https://perma.cc/BU2X-F9E8]

[54] *See* James Pattison, "From defence to offence: The ethics of private cybersecurity", *European Journal of International Security*, Vol. 5, Iss. 2, 233-254 (June 2020), https://www.cambridge.org/core/journals/european-journal-of-international-security/article/from-defence-to-offence-the-ethics-of-private-cybersecurity/4DE2DD7F39CC66E3703943D4D65999FF [https://perma.cc/5B5A-XREX]

[55] *See* Kevin C Desouza, Ahmad, Atif, Naseer, Humza, and Sharma, Munish, "Weaponizing information systems for political disruption: The Actor, Lever, Effects, and Response Taxonomy (ALERT)", *Computers and Security* 88 101606-101606, https://findanexpert.unimelb.edu.au/scholarlywork/1413022-weaponizing-information-systems-for-political-disruption--the-actor--lever--effects--and-response-taxonomy-%28alert%29 [https://perma.cc/UR42-G349]

Subversion, Information Operations and 'Deep Fakes', authors Paterson and Hanley state "this [voters being forced to question whether special interests or foreign powers impact election outcomes] is highly damaging for the political legitimacy of democracies".[56] Political warfare has begun to increasingly rely on social media and it is no longer enough to simply be on the defense. Unfortunately, with rapid developments continuing to occur across the planet, we cannot expect technological warfare practices to die down anytime soon, so both defensive and offense moves are the only way to secure our country's sacred notions of democracy.

In the aftermath of 9/11, there was overwhelming national support to track down Osama bin Laden, the perpetrator and mastermind behind the attack that killed 3,000 Americans in 2001. To do required years of careful planning based off of small, questionable bits of intelligence with no guarantee that the paths would lead to bin Laden's location, capture, or death. Without the resources of social media tracking, data records on phone calls, and triangulation, it is possible that we still would not have the relief and sense of justice felt around the nation at the news of bin Laden's confirmed death. It is important to recognize this event as one that demonstrates the great benefit that data points can bring to the nation and see the benefits of being proactive.[57]

Beyond the threats to national security, corporations also have an obligation to utilize their extensive resources for all-around good. This has no long-standing legal precedent, but simply is a moral and ethical code for humanity to live by. Additionally, since the social climate at the moment is so consumer-driven and sensitive to social issues, corporations are put into the unique position where they must vocalize their companies' perspectives and values. They are not afforded the privileges of staying silent, but rather must risk isolating certain populations by becoming vocal about key social issues. Every search, posting, keystroke that has ever been made is stored by these companies to be bought, sold, and used for various purposes – often without the user's explicit awareness or consent. While this may have been acceptable in the past, the ethics and morality behind the behaviors of these major companies is now being challenged by users and even company employees. With access to such tremendous amounts of information, technological, and financial resources, the pressure for social media companies to be advancing societal goals is mounting.

The developments of modern technology have enabled inexpensive video capture, which links to global networks such as YouTube, Instagram, and Snapchat, making news in one area expand to a global audience. This in turn has transformed brands to be increasingly dependent on user interest and social trends. The traditional forms of media that were popular in the past such as newspapers, radio, and television are all now simply venues to draw attention to the digital media that is mobile, online, and omnipresent. These new forms of digital technologies have created a population that is heavily connected, outspoken, and in hard pursuit of products that align with their personal interests. Recently, human rights injustices in America have been exposed and attacked and strategic communications and public relations industries have had to make their social stances clear in order to maintain relevancy and consumer support. In the past, brands would typically remain relatively silence in terms of social issues in order to avoid repelling potential consumers. However, circumstances are now the complete reversal: Brands are forced to make vocal social statements in order to avoid repelling eagle-eyed consumers in pursuit of brands that support their ideals and values.

The consumerism aspect of data mining and collection should come second behind the right to make independent political decisions that are well-informed and grounded in accurate truths. It is a questionable practice to monetize and sell data in and of itself, to do so with the intent of advancing certain political agendas forward also violates deeply rooted moral and ethical responsibilities. While both are dubious, there is a large difference between selling someone's Christmas shopping browsing and scrutinizing large clumps of data bytes in order to determine who would be most easily swayed to vote for a certain political candidate. As we collectively begin the delicate process of combatting violations of user privacy by large corporations as well as continuing to adhere to our proud standards of democracy and freedom of expression, it must be characterized by legislation that is relevant, specific, yet timeless. These are largely uncharted waters and have created somewhat of a moving target situation. Nonetheless, there progress cannot be made without arrows aimed towards the target. The past hearings in the Senate have been beneficial in that they represent the beginning of grasping control of the largely untapped powers of the Internet, but it is imperative that it is indeed recognized as only the beginning in order to maintain the safety and security of our cyberspace for all citizens.

Legislation is important to maintain the delicate balance of rights to individual privacy and advancing the greater security of our nation for all citizens, but the role that major Internet corporations play in ensuring the access to said

[56] *See* Thomas Paterson and Lauren Hanley, "Political warfare in the digital age: cyber subversion, information operations and 'deep fakes'", *Australian Journal of International Affairs*, Vol. 74, Iss. 4, 439-454, (March 10, 2020), https://www.tandfonline.com/doi/abs/10.1080/10357718.2020.1734772?journalCode=caji20 [https://perma.cc/WNX9-AM8B]

[57] *See* Mark Bowden, "The death of Osama bin Laden: how the US finally got its man", *The Guardian*, (October 12, 2012), https://www.theguardian.com/world/2012/oct/12/death-osama-bin-laden-us [https://perma.cc/6YYY-NZM6]

data is also vital. The government does not own Google, Facebook, Microsoft, or Twitter. Instead, it relies solely on the establishment of relationship with between federal government agencies and major tech companies to discover means that are beneficial for both parties. If the government were to over-legislate and forbid all data surveillance, then Homeland Security suffers harm and struggles to carry out critical operations with high national security stakes. If they under-legislate, all citizens are at risk of being digitally exploited and the United States succumbs to the tech titans. The best strategy at this point in time is to recognize data to be the sine qua non that allows the United States to be a nation of power and authority, ensuring democracy and security for itself and its citizens. Data has huge value, the root of the issues involving security, privacy, and monetization of data is to determine how this value can best be utilized for the wellbeing of all persons. Data scooping is the innumerably valuable tool that has proven itself within the last decade to be the factor that leads to determining presidency or finding the next Osama bin Laden. While exploitable and posing major risk factors, the harsh reality is that data mining and technological warfare will only grow in the coming years.

There is already so much data on servers that capture and store data from across the internet, it will never fully disappear. These servers are where data is collected, then manipulated and sorted. While they vary in terms of size, these "server farms" are located all over the world, the largest being in China and occupying 6.3 million square feet.[58] There is so much data in existence being stored in China, Russia, North Korea, and more; if the United States opted not to legislate the way data is handled, then the country would be extremely vulnerable to these countries. A hard pill to swallow, but privacy in the modern age is likely going to be no more. Users are not forced to sign up for Facebook, Google, or mobile banking accounts. They are told that any information they put in can be used and made public, but the consumer mindset is often willing to trade personal information or privacy because of convenience or the belief that it isn't harmful. The world will not arrive at the unanimous consensus that major tech should be eliminated or forced to submit to all government orders. Rather, we must understand that this age of informational data presents some of the biggest changes of how humanity functions. There will be mistakes made along the way, but moving forward to determine how to reconcile the huge value of data, need to protect democracy and privacy, and utilization of technological advancements to our national and global benefit will only occur through a recognition of the vital and omnipresent role data plays in our modern society.

--0--

How to Cite this Article

Taschner, J. B. (2020). Data Profiteering: Corporate Social Responsibility and Privacy Law Lost in Data Monetization and National Security. *American Journal of Trade and Policy*, *7*(1), 37-50. https://doi.org/10.18034/ajtp.v7i1.484

[58] *See* Mike Allen, *"And The Title of The Largest Data Center in the World and Largest Data Center in US Goes To…", Datacenters.com,* (June 14, 2018), https://www.datacenters.com/news/and-the-title-of-the-largest-data-center-in-the-world-and-largest-data-center-in [https://perma.cc/5VNK-2MT3]