Vassar College
Digital Window @ Vassar

Senior Capstone Projects

2016

Digital advertising regulation and issues of internet privacy

Zachary Rippe
Vassar College

Vassar College

DIGITAL ADVERTISING REGULATION AND ISSUES OF INTERNET PRIVACY

A Senior Thesis submitted in partial satisfaction of the requirements for the degree

Bachelor of Arts in Media Studies

By

Zach Rippe

Faculty Advisers:

Professor Bill Hoynes
Professor of Sociology and Director of Media Studies

Professor Dara Greenwood
Associate Professor of Psychology

Submitted: April 22, 2016

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION – WHAT IS GOING ON?

“There are many great things about the new media environment. But when companies track people without their knowledge, sell their data without letting them know what they are doing or securing their permission, and then use those data to decide which of those people are targets or waste, we have a serious social problem.” – Joseph Turow, *The Daily You*

I became interested in issues of online privacy and anonymity while taking a Media Law and Ethics course abroad in London. Among other topics dealing with things like copyright and intellectual property, we examined the extent to which companies and advertisers track and personalize everyone’s online experience. This interest was further expanded upon in my “Media Theory” course at Vassar last year. Companies and their various advertising platforms, the most prominent being Google AdWords, not only allow advertisers to appeal to specific demographics, but also track users according to what sites they visit, where they click and what they buy. This later affects the ads they see. With sites like Facebook, where we access content for free, we are not simply users or customers but products. Companies sell our data for profit, defeating the notion of the Internet as a democratized space where “passing” is plausible and anonymity is the norm.

I hope to work on understanding methods of digital advertising and online privacy because I want to know more about how advertisers dictate users’ internet experiences and control how they move through the online realm, in order that my readers may better understand the impact advertising companies have on online space and the limits of privacy they define for users on the web. To tackle these problems, it is important to conside a few key questions: What legislation currently exits, and in addition what legislation can and should be proposed to help regulate this rapidly developing industry? What are the idealistic and realistic solutions to the commodification of the digital world and in turn the digital lives we lead?

Even when we “create” content, we market ourselves along side the products we propagate and advertise for the purpose of a further proliferation of these products and advancement in the professional field. Online, we are trapped in a vicious cycle that reduces our name to a brand in the best-case scenario. While we acknowledge the necessity of this, we also downplay the reality that the ever-accelerating circuits of images and feelings that we are reduced to online have been commoditized in themselves. The way we navigate the web and the online world in general may soon be as natural as navigating the actual world. In order to maintain our privacy, our online rights, our agency and keep ourselves free from exploitation for capital gain, it is important we know how the internet operates, how digital advertisers control how we navigate this digital space, and what we can do to create a more democratized online future.

To do this, I need to gauge not only the level of people’s awareness regarding the digital marketing industry’s practices, but also the extent to which they care; the extent they are “creeped out.” Do they care enough to actively fight for their anonymity? What would it take for them to care enough to act? I am looking critically at practices of digital advertising and the effects they have on internet users’ privacy, anonymity and comfort-level while navigating the online sphere. I hope to examine the existing legislation put in place by the Federal Trade Commission (FTC) and make clear how it favors marketing firms and puts the onus on individual users and companies to self-regulate their online experience.

I know that Internet sites need money to run. Users do not want to pay for content, making advertisements the realistic, plausible solution. How would the Internet change/be regulated if it didn’t have this sort of revenue-based system in place? In the end, the main question I am asking becomes: What steps can be taken, both in regards to the individual’s experience and the overall structure of the online world, to not only subvert this digital advertising culture but change it for the betterment of our online futures? Carefully regulating the industry to ensure users’ privacy and rights, provide mandatory corporate transparency and increase online literacy to ensure that subversion for those who desire to seek it out, an inherently plausible and well-rounded approach, is the desired solution.

Other work has been done by scholars like Joseph Turow and Eli Pariser to explain what these companies do, how they and marketing practices in general are shaping our online experience and turning us into products rather than consumers, and steps we can take towards a better, more transparent online future. In addition the Pew Research Center provides accurate, relevant data and research concerning peoples’ online awareness, the extent to which they perceive they have control over their online experience, and the level of confident they have in the security of their personal, private information.

In looking critically in the role of media in our lives, it is no secret that the amalgamation of the real and digital worlds is one of the most pressing media-related issues in our society today. This fusion is inevitable. To prepare ourselves, we must look critically at our relationship with this technology to further understand how it affects and changes us both as individuals and as a society. The main purpose of my project is not to find groundbreaking research, but rather to explain and present an issue to a group of people in such a manner that it raises awareness. The problem with digital advertising stems from a lack of common knowledge; lack of a common discourse. People aren’t talking they are only clicking.

We need to start a conversation that can only be had with more familiarity around the subject. We need to better understand what is being done to our "online profiles" which will, more and more, become an extension of ourselves in order to understand how the medium and digital world are changing the way we think and interact with one another.

Marketers' goal is to figure out individuals' buying impulses and they are doing it more accurately than ever before. They are in effect destroying traditional publishing ethics and performing highly controversial forms of social profiling and discrimination through the customization of our media content. Joseph Turow continues:

> "The future belongs to marketers and media firms that learn how to find and keep the most valuable customers by surrounding them with the most persuasive media materials… this allows publishers to auction and media agencies to 'buy' individuals with particular characteristics, often in real time. That is, it is now possible to buy the right to deliver an ad to a person with specific characteristics at the precise moment that that person loads a Web page."[1]

Advertisements and discounts also become social status symbols, as certain products and services advertised to certain demographics of users affirm people of their social position. "Your sense of the world's opportunities may be narrower than that of someone who is feted with ads for national or international trips and luxury products." Those worried about others receiving more advertisements for luxury products and services than them may feel as if they are "falling behind in society's estimation of [their] worth."[2]

[1] Joseph Turow. *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth* (New Haven: Yale UP, 2011). 5.
[2] Turow, *The Daily You,* 6.

There is a shift coming in the way that information itself is produced. This is seen in the production of news. We no longer have to buy a whole paper to go to a specific section. The cost of producing and distributing all types of media continues to fall closer to zero. At the same time, we are seemingly overwhelmed with choices of what to pay attention to and continue to suffer from what Eli Pariser calls "attention crash." We rely more heavily on human and software curates to determine what news we should consume.[3]

We are entering a world of customized content where personalized ads are subtly meshed in with soft news and entertainment is tailored to particular users' needs and reputation.[4] We are told what to choose, what to like, what people we should be like. Gone is growth and discovery. We pigeonholed ourselves and before we know it we are told what to like and how to discover and learn, rather than who we are and who we will become.

As personalized filtering continues to get better and better, we begin to devote less and less energy to choosing what content we want to see and access. Thus we are subtly forced to trust the companies who personalize our experience to synthesize who we are digitally through extensive data that they research and trade with one another. The future is even scarier. There are a variety of apps and start-ups that are working to use invasive technology like facial recognition to identify users as soon as they go on their computer.[5] Noticing someone online will soon be as easy as noticing someone on the street. Businesses may also begin tracking users around the globe with specially designed chips. Theorist David Wright claims that every manufactured product, from clothes, to money, to appliances, to carpets and cars will eventually be embedded

[3] Eli Pariser. *The Filter Bubble: What the Internet Is Hiding from You.* (New Haven: Yale UP, 2011), 51.

[4] Turow, *The Daily You,* 7.

[5] Pariser, *The Filter Bubble,* 196.

with intelligence networks of tiny sensors and actuators. Something that some have already dubbed "smart dust."[6]

Personalization may feel comforting; as if we are right at home and everything is presented to us on a silver platter and we will immediately love and consume all of it. But down to our identities themselves, we are not creating anything anymore. As Pariser puts it, "You live in an equilibrium between your own desires and what the market will bear. And while in many cases this provides for healthier, happier lives, it also provides for the commercialization of everything – even of our sensory apparatus itself."[7] We run the risk of losing more than our privacy. We may lose our identity and self worth all together. This is something that needs to be addressed.

To begin my thesis, I will first examine the history of the Western advertising industry throughout the 20th century to better understand how we got where we are today. I will then transition into the history and inner workings of Google, a "Big Data" corporation with a monopoly over data and the majority of the digital world. Then I will examine the acceleration of capitalism and consumer culture in recent history. I will see how and why public-private ties were developed and how they reflect the self-regulation, company-oriented digital advertising legislation that gives companies free reign to implement their own lenient policies that benefit private entities over consumers. Next I will transition to the FTC's laws and regulation in comparison with their EU counterparts to highlight the differences between a self-regulatory system and that of centralized, user-focused regulation and its possible implications on trade and U.S. policy. I will conclude with an analysis of modern users' sentiment through the lens of the recent Pew Research Center poll on security and privacy in the United States. Through this

[6] Pariser, *The Filter Bubble,* 198.
[7] Pariser, *The Filter Bubble,* 215.

analysis, I hope to prove that it isn’t just what is happening now that hurts us as a society, but rather what will happen if these powers go unchecked. Something needs to change or we risk losing our identities, as we know them.

CHAPTER 2: HOW WE GOT HERE
A brief history of the practices and tendencies that define the modern digital advertising landscape

Publishing methods once considered traditional and ethical are having their methods called into questions due to modern, digitally based practices used by media buyers and third-party digital advertising firms. Media outlets in the digital sphere are being pressured into adapting their content to meet the needs of advertisers who utilize controversial methods of data collection and analysis. This tactic has evolved to become a quite effective form of social profiling that customizes users' media content based on digital profiles that many do not even know exist.[8] To exclusively fault this era, this generation, this new digital technology, however, would be a misstep. A detailed examination of evolving advertising practices throughout the second half of the twentieth century shows that the development of the Internet was in fact the final step in a long, intricate hunt for something that was once only dreamed about: individualized social profiling and precise, personalized, cumulative user data.

As Joseph Turow points out in his 2011 book, *The Daily You*, "the idea that individuals would hold power over media destinies in the twenty-first century got a lot of traction [in the 1990s]."[9] This assumption, drawn from Nicholas Negroponte's 1995 work, *Being Digital*, does have a degree of truth to it, yet it is extremely optimistic and does not take into account the feelings, perceptions and practices of advertisers and media-buyers in the latter half of the twentieth century. The 1980s and 1990s, for example, saw a shift where companies chose to separate their media planning and buying into stand-alone

[8] Turow, *The Daily You,* 2.
[9] Turow, *The Daily* You, 14.

businesses within the advertising industry. Eventually third-party companies developed and grew to fill this role. New divisions developed increasingly detailed and accurate models to measure hard data from users' actions online, as well as consumer responses, trends and behaviors.[10] Why would these agencies choose to split? Why was there so much animosity in the industry in the first place? Without a look at history of these processes beginning at the early decades of the century, it is difficult to understand why and how these shifts came to be.

At the turn of the twentieth century, advertising agency executives had trouble grasping the practice of media buying. Thus, these "media-buyers" were often revered in the industry. At the height of radio from the late 1920s through the 1940s, advertisers literally owned the programs they chose to sponsor. The role of the media departments was often to simply produce these programs for the advertisers' clients, giving them complete control. As the popularity and accessibility of the television grew throughout the 1950s, the first real shift took place. Programs on television were owned by networks and local stations rather than advertisers. Now advertisers simply purchased slots within and around shows based on how may viewers were tuning in.[11] For the first time, the number of viewers and eventually their demographics became an important, if not vital, aspect of successful advertising. With this new technology came the potential and desire for a collection of mass data and a careful examination of group tendencies and demographics.

By the 1960s, this process of finding print space and buying air and broadcast time for clients became simple enough to shift their focus. The goal was now to be more efficient and specific with gathered data and modes of doing so. The advancing technology

[10] Turow, *The Daily* You, 20.
[11] Turow, *The Daily* You, 21.

and increased manpower led to the development of new channels and modes of advertising direct mail advertisements and niche magazines designed to target specific demographics. Most work could be done by recent college graduates who could work for cheap wages and afford to spend hours "[poring] over boring television ratings and periodical data in conjunction with advertising charges to determine the key measure of an ad vehicle's efficiency."[12] This measure, dubbed "CPM" or "cost per million" detailed the price for reaching a thousand members of a target audience via one specific outlet. With newly standardized terms and metrics, the industry now saw media buying as pedantic, yet extremely critical to monetary success.

Through the late 1960s and 1970s, the vitality of media-buying practices led to the emergence of independent media-buying companies, thus marking the very beginnings of the modern digital advertising landscape. At first, this practice was not widely accepted, but the establishment of Mercury Media as a separate media-focused entity in the United Kingdom in 1975 helped bring the practice into the focus of the mainstream business world.[13] Advertisers in both the UK and US feared the possibility of client conflicts, yet agencies argued that competing clients would not be aware what media their competitors were buying. They also countered that an agency devoted solely to media-buying was the most effective model for taking care of clients needs and developing creative research, planning and buying methods.[14] As the number of TV channels grew, there became a more opportunities for product placement, making the task itself much more daunting than it had been in the early years of television. This increased gathering of data lent itself to a

[12] Turow, *The Daily* You, 21.
[13] Turow, *The Daily* You, 23.
[14] Turow, *The Daily* You, 26.

closer examination of and thus a greater emphasis on specific demographic tendencies. For the first time, advertisers were afforded the luxury of discovering who people were and what types of people were interested in particular products and services. Thus a much larger percentage of ad budgets were going to media spending as this practice cemented itself as the primary concern for most major companies.[15] Still, companies operated under the assumption that demographics could be all telling of where to direct their efforts. In reality, these groupings offered generalizations that still required a lot of guess work and thus a substantial amount of uncertainty.

By the late 1990s, the consolidation of this media buying had reached a stage where only the top four or five media companies could maintain their power and status while they looked to keep expanding and swallowing up lesser entities.[16] "New media" companies boasted about their extensive resources and research, along with their comprehensive knowledge of new technology. This wherewithal could be used to optimize advertising expenditures to reach specific intended audiences across multiple mediums. Critics, however, discredited these claims as they felt these companies were simply making up this new "science." As Turow explains through the eyes of critics: "Building optimization weighs into formulas based on these ideas simply lent bad research and executives' guesses a spurious aura of quantitative legitimacy."[17] While primitive and inaccurate at the time, these new optimization strategies would later prove to lay the groundwork for the future of marketing in an increasingly digital world.

[15] Turow, *The Daily* You, 28.
[16] Turow, *The Daily* You, 29.
[17] Turow, *The Daily* You, 31.

Weighing judgment calls and experience over concrete ”scientific” strategies may have seemed obvious to advertisers in the 1990s, but gradually, the scale began to tip in the opposite direction. In order to draw big money operations, media-buying firms had to highlight their quantitative knowledge of their audience and accept accountability. More importantly, this offered a method of demonstrating clear, quantifiable results.[18] It was not so much the developing system itself, but a fear of the unknown; the unknown research methods, the unknown medium and the untapped potential for something that an older generation of advertising agencies and media buyers did not yet understand. These evolving marketing practices that grew over the course of the 20th century were organically developed by firms themselves. By the 1990s, they had everything in place except the confidence in a perfect medium with which to carry out their idealized strategies. While developing technology allowed for more precise data that led advertisers closer to the specific user information they wanted, Cable TV still had to work with groups, guesses and assumptions. The desire for actual, individual data grew as advertisers feverishly looked for ways to obtain such information, yet lacked the technology to do so. The development and understanding of the Internet was the final step, not the initial one.

The transition into the digital world was hampered by the expansive unknown of the digital sphere and a lack of knowledge and framework for both how to develop reliable metrics and what they would come to mean. These systems never existed and thus it was virtually impossible for this generation of digital marketing pioneers to immediately gauge their effectiveness. While running a pay per click advertisement campaign for a company this past summer through Google AdWords, I learned that it would take about a year to

[18] Turow, *The Daily* You, 33.

properly evaluate the data I collected. This was with all of the resources, help and knowledge I could possibly hope for. Making sense of data that had never been tested before must have felt at times hopeless and downright impossible. What metrics are most effective? Do they differ for different markets? The development and implementation of these metrics was initially a process of trial and error – granted one that took place over a decade rather than several months. The algorithms we have today are a direct result of a refining of these trial and error processes. They have been legitimized by little more than internal trial and error and time.

Media-buying agencies and advertisement developers in the 1990s thus initially saw their foray into the online realm as low budget and experimental. Rather, they wanted to probe into a future where things could be much more effective than in the past, framing their work as "getting a head start" rather than panicking about the new medium.[19] The "click" became their first great ally, as it was pure quantitative proof of value on the Internet. Now, advertisers and media-buying companies could see how many people clicked a specific ad or webpage, as well as when they clicked. This was a stark departure from the pre-digital days where they had to rely much more on uncertain mass demographics and guestimations. The potential of this medium would allow advertisers to reach out to new audiences and markets as well as have an in on individual users' tendencies.

Still, a lack of knowledge, even surrounding the click specifically, proved a flaw that initially raised more questions than answers. Because media-buying decision makers were almost always removed from those involved with or knowledgeable about the Web, they

[19] Turow, *The Daily* You, 36.

hesitated to tap into its potential. They refused to see the Web as something that would ever become a serious medium for branding and advertising beyond direct, basic forms of marketing.[20]

Internet publishers, wanting a piece of the monetary pie, prodded and pestered media buyers. They hinted that users would not be paying for the majority of their online content, a detail that holds true today despite the best efforts of advertisers and media corporations. Users, then and now, do not want to pay for content. In a digital world that offers both options, however unethical they may be, a majority of users will always opt for free content. There have been past examples of premium content on sites like ESPN that simply weren't successful. In reality, only top tier companies with excellent reputations would be able to get away with having users pay for access and services. Alternative sources would remain free either in principle or out of necessity.

In the meantime, advertisers experimented with a host of new strategies, including: developing new ways to count and measure clicks, creating different ad formats and technologies to spike clicks on ads, attempting to understand why visitors went to their site so they could target them directly, joining firms that charged advertisers for people's clicks on ads, and traced what visitors tendencies were on specific sites. Limitations beyond the understanding of media-buyers and major markets included the fact that in 1994, the Web was mainly a text-based medium.[21] No one could see pictures, sounds and videos without downloading them specifically. Media buyers still were weary about investing so much into a product they did not understand. With the Web, they did not feel like they were in control. Did they really want to be tricked by these tech-savvy youngsters?

[20] Turow, *The Daily* You, 37.
[21] Turow, *The Daily* You, 38.

The development of the web browser in the early 1990s helped revolutionize both the Web and online marketing worlds through its accessibility and increased technological capabilities. While the first prototype was designed in late 1990, the fall of 1993 saw the introduction of Netscape's first browser, the NCSA Mosaic.[22] The introduction of web browsers allowed for pictures, sounds and graphics to seamlessly and instantly be incorporated into a user's web experience. This made advertisements all the more powerful and relevant. Now the general public could access and navigate the web at ease, making the experience one of leisure rather than that of an intellectual strain. The first Internet ad ever was sold by the Global Network Navigator Company to a Silicon Valley law firm in September of 1993. Colorful banner ads across pages became the earliest popular mode of advertising. AT&T bought the first ever banner ad from Modern Media in October the following year.[23] While companies toyed with a variety of different methods for charging visitors to enter specific sites, they all crumbled under the inevitability of the notion that the vast majority of content on the Internet would be accessible for free. Thus there was a desire and necessity from both Web publishers and advertising agencies to make this work.

Web publishers thus began to develop increasingly accurate ways to measure clicks and informational data. "Impressions" were measured every time an advertisement was sent to an individual who had clicked on a site's page. Eventually, one could devise a method where they divided clicks by total number of impressions to achieve a "click-

[22] "Bloomberg Game Changers Marc Andreeseen." http://www.bloomberg.com/video/67758394-bloomberg-game-changers-marc-andreessen.html, 2014.

[23] James Bourne. "Online Advertising: A History from 1993 to the Present Day [Infographic]. http://www.marketingtechnews.net/news/2013/sep/11/online-advertising-history-1993-present-day-infographic/, 11 Sept. 2013.

through-rate".[24] At this stage, publishers stressed their ability to tell media buyers and advertisers as much as possible about site visitors who might or might not click a banner ad. For advertisers, anonymity was the problem, as they could not figure out how to market to these people. Advertisers were scrambling for information that they did not know how to interpret. They needed third-party companies to tell them "how many people are logging onto their sites, who they are, where they're coming from, what they're doing once they get there and how long they stick around."[25]

Inevitably, companies like the Internet Profiles Corporation developed to meet this demand. Internet Profiles Corporation, or "I/Pro", boasted names like Hearst, Netscape and Playboy as customers. Different services like I/COUNT and I/AUDIT would let site owners monitor their sites visits, pages viewed, geographic location as well as analyze results and deliver monthly reports. Business owners were worried about the possibility of fraudulent data. Websites and I/Pro could only track sessions, not individuals, meaning they couldn't be sure whether clicks represented particular visitors. Owners also increasingly had to deal with the issue of web companies themselves trying to draw visitors from others sites to their own so they could sell ads at high prices. Much of this was done with the money they received *from* venture capitalists themselves.

By late 1994, a new invention had arrived that would mark the beginning of the shift of power in the digital advertising sphere, and the Internet in general. The Cookie, created by Lou Montulli, was described by Turow as something that "would ultimately do more to shape advertising and social attention on the Web than any other invention apart from the

[24] "AdWords" *Google AdWords.* Google. November, 2015.
[25] Michael Krantz, "The Medium Is the Measure," *Adweek,* November, 2015.

browser itself."[26] Montulli was working for Netscape Communications and was attempting to develop a more effective shopping cart that could keep track of multiple items a shopper would theoretically set aside for purchase. In the existing model, each click would be interpreted by the system as a different individual making a purchase. Thus people could not buy more than one thing at a time; the existing system stored personal information in the web address and URL.

Montulli developed a small text file that could be placed on a visitor's computer, giving them their own unique identification code. The next time this person visited that site, the browser could recognize the cookie and thus build a unique profile based on past and present visits. More specifically, the data revealed where the user of the computer had previously clicked, what they had purchased and what they placed in their shopping cart even if they did not end up buying it.[27] Montulli expressed mix feelings about his discovery, noting that he and his co-inventor John Giannadrea had realized the cookie's potential for becoming a universal tracking system[28] and had originally tried to limit what information would be sent back to the corresponding site. Naturally, Netscape installed a cookie-placement capability into their newest Navigator Internet browser at the end of the year. Microsoft did the same to their Internet Explorer browser in 1995 to remain competitive.

Still, advertisers were unsatisfied. They felt that while they could see hard data about a user's visit, they still could not measure the specific characteristics of an audience. To fill this void, audience-side companies began to emerge and bid for media buyers'

[26] Turow, *The Daily You,* 53.

[27] Schwartz, John. "Giving the Web a Memory Costs Its Users Privacy." The New York Times. September 4, 2001. Accessed November 17, 2015. http://www.nytimes.com/2001/09/04/technology/04COOK.html.

[28]Turow, *The Daily* You, 54.

research money with the intention of creating an online equivalent of the Nielsen's television ratings. In 1996, Procter and Gamble decided to use audience-side ratings rankings to solicit proposals from websites to place banner ads for sites built around their products, agreeing to base advertising fees on how many times an ad was clicked and subsequently sent visitors to a P&G site. Some large companies like Yahoo! joined in, but others like AOL felt with their capital and knowledge could afford to abstain.[29]

Other agencies put their efforts into more creative, visual advertisements, crafting full-page ads, animated ads and even downloadable screensavers. Agencies and developers sometimes crafted intermediate websites with flash animations or java applications that allowed users to play company-sponsored games without ever leaving the websites. There was now a growing pressure to present data on the part of advertisers as major advertising agencies became involved.[30] Along with the creation of separate digital advertising departments within companies and firms, the standardization of ad sizes allowed for a simpler, more uniform system that again highlighted a further legitimization of the industry and its process.

When Netscape launched the Navigator 2.0 in 1995, it seemed to heed Montulli's warning – the browser gave users the ability to view the existence of a cookie in a visitor's browser. However, only the site that created that cookie could read or change it. While seemingly transparent for the time, this gave users little to no control over how they were being tracked. It simply let them know both that they were and by whom. At the same time, marketing entrepreneurs kept at their work. They realized that if they could receive permission to place cookies across multiple sites, they could track what individual users

[29] Turow, *The Daily* You, 49.
[30] Turow, *The Daily* You, 54.

did after they obtained the cookie on a certain site, tracking their behavior throughout their online experience. “If a cookie were detected at one of the related sites, the marketers could serve an ad to that individual’s screen in sync not only with the topic of the current website but with those visited previously.” These cookies were dubbed “third party cookies” as they were controlled by an agency or entity separate from the website on which they appeared. These are the cookies that every-day Internet users in the US are often advised to delete. Various anti-spyware and anti-virus programs, as well as some computers’ default privacy settings now automatically block these third party cookies. This practice has become so commonplace that some analytics firms today advertise using exclusively “1st party cookie technology” on their sites.[31]

Not only would the subsequent data be added to the cookie, but revenues were also often shared with the participating sites. Thus marketers began to attempt to create ad networks, incorporating as many sites as possible. By fall 1996, this became so popular that even content providers offered the ability for advertisers to buy ad space across their domains and through cookies determine whether ads were going to new or repeat visitors.[32] However, with these increasing possibilities came the problem of scale. In more traditional media, buyers for major advertisers would buy large numbers of peoples’ data through just a few firms. However, on the Internet, these audiences are scattered much more widely throughout the web, meaning several websites would only distribute a relatively small number of people. This pushed certain sellers to separate themselves from

[31] "Third-Party Cookies vs First-Party Cookies." Opentracker. Accessed November 27, 2015. http://www.opentracker.net/article/third-party-cookies-vs-first-party-cookies.
[32] Turow, *The Daily* You, 55.

the competition by providing huge numbers of users' data across literally thousands of sites.[33]

From this perspective, users were (and still are to a degree) reduced to a number, a statistic or a general sentiment that helps define a trend. It is only through this intense filtering and fractioning process of the online world itself that allows for not only a personalization of content, but a desire for this extremely private, extremely individualized information as well. It is not people, but rather machines that catalogue users' information, making the process, at least then, much less personal than it actually felt.

Pushback arose from places like the Internet Society's Internet Engineering Task Force, who identified third-party cookies as a considerable privacy threat. This nonprofit organization provided an early attempt to give users some direction and education on internet-related standards and policy. Both Netscape and Microsoft web browsers also developed the ability for users to change their cookie preferences manually. However, they could not automatically choose to stop cookies.[34]

Obviously choosing to regulate in this fashion was advantageous to marketers, web developers and all those involved in the process of buying and selling data in the emerging industry. However, it showed the continuation of a culture that put the burden on the user to self-regulate their privacy and overall online experience. By 1997, the new Netscape browser, the Navigator 4.0, gave users the ability to either reject all types of cookies, some types or none at all, again shifting responsibility to the user. However, Montulli, himself the

[33] Turow, *The Daily* You, 56.
[34] Turow, *The Daily* You, 57.

inventor of the cookie and an active member of the IETF correctly theorized that the effects would be minimal as users did little or nothing to stop the flow of cookies.[35]

Various reports began to emerge that publicized the debate of online privacy, exposing exactly what cookies and these marketers were capable of. A 1996 *Mac Week* article showed that cookies and JavaScript simply on the Navigator browser on Macs could obtain a user's email address, real name and activity from its cache file. A 1998 report from The Center for Media Education entitled "Web of Deceit" showed how marketers used websites to pull information from young users and their family members. This report proved immensely influential and led to the "Children's Online Privacy Protection Act" (COPPA).[36] This act prohibited websites from receiving personal information from children under 13 years old without their parents' consent. Hence the commercials on TV and online prompts upon navigating to a webpage that asked kids for their parents' permission for "safety" reasons.

Despite this legislation and constant pushback, Web publishers and third-party advertisement networks did not stop accelerating and developing the digital marketing process. As the Internet expanded exponentially and the "science" behind digital advertising statistics and practices became more of an actual science, they had increasingly more opportunities to get detailed information by analyzing click habits across sites. This competitive cross-site clicking, coupled with a growing number of ad networks, spurred increased competition that lead to more creative, in-depth analyses and in turn descriptions of users in ways that advertisers would benefit from.

[35] Turow, *The Daily* You, 58.

[36] "Children's Online Privacy Protection Act." Wikipedia. Accessed November 23, 2015. https://en.wikipedia.org/wiki/Children's_Online_Privacy_Protection_Act.

The development of the “web bug” or “web beacon,” a small, invisible graphic that is usually one pixel by one pixel in size, was created to make it easier to follow visitors across pages. Previously, ads were not stored on the same computer servers as the pages of the websites onto which the ads were served. Whenever a user clicked on a page, an advertising image was downloaded that required the browser to request the image from the server that was storing it. This request would include the page on which the ad would appear. Thus, the ad network would be able to know which pages the visitor had browsed and subsequently store that information on either one of that person’s cookies or on the network’s computers themselves.[37] These bugs could also exist without ads. They could also trigger when placed in graphics, gathering all information about a visitor while being invisible at the same time. Here the purpose was not to advertise to users, but simply gain valuable information about their browsing tendencies.[38]

By the late 1990s, some advertisers were still extremely hesitant to join the industry. According to an *Advertising Age* article from August 1998, CEOs and big media buyers were still skeptical of the underdeveloped practices regarding data and statistics. [39]Still, there grew an increased seriousness to learn about how to interpret this information. Companies began to hold retreats, conferences and educational sessions to discuss and learn about online marketing practices.

P&G, for example, took an in depth look at how to configure the Web in such a way that it could one day replace TV as the company’s main venue of advertising. As Turow

[37] Turow, *The Daily* You, 60.

[38] Smith, Richard. "The Web Bug FAQ." The Web Bug FAQ. November 11, 1999. Accessed December 1, 2015. https://w2.eff.org/Privacy/Marketing/web_bug.html. - Found via the Electronic Frontier Foundation

[39] Turow, *The Daily* You, 61.

described, “The promise of the Web was that a TV-like ad on a site could stir emotions that would reinforce branding while encouraging clicks that would lead people to learn more and leave their e-mail addresses for coupons and other ways P&G could address them.” Still, P&G quickly learned that while the Internet had tremendous potential for growth and monetary gain, it was not yet at that stage in its development. Click through rates, while still incredibly low when considered effective, were at less than one half of one percent, a radically different statistic from that of TV ads. A 2001 article from *Industry Standard* noted that 12 percent of media consumption took place on the Internet, yet it accounted for less than three percent of overall US ad dollars.[40]

There was tremendous potential for the digital marketing industry, however it was growing quite slowly. In 2002, however, Google was born. The company joined with thousands of small marketers that saw it as a practical, efficient and more measurable way to lead consumers to clients’ products than display advertising. Google made 2.08 billion dollars in its first year. With the rise and spread of broadband, there were vivid commercial possibilities available by the late 2000s. By 2009, the top 100 consumer advertisers in the US spent around 90.7 billion dollars on advertising. Around 15% of buys shifted to digital media in 2009 and the trend has been growing since. The reallocation of money to the web, video games and mobile devises has reinforced this process of devaluing traditional ad vehicles like print newspapers and magazines as well. In essence, the Web was developing too fast for the marketers’ own good. As culture caught up with technology and transferred it into a popular online sphere that extended beyond desktop computers, marketing executives were finally beginning to master the processes and data that lie behind the

[40] Turow, *The Daily* You, 63, 64.

lucrative world of digital marketing, a combination that has allowed their money to grow exponentially along with the technology that drives it.

CHAPTER 3: GOOGLE
An examination of modern digital advertising practices through the lens of a dominant corporate entity

Sitting at the top of the digital advertising and big data world is Google. The company, started in 1997 by Larry Page and Sergey Brin, has grown exponentially over the years and has come to dominate almost every spectrum of the digital realm. By 2013, Google held nearly 70 percent of the search engine market and 97 percent of the mobile search market.[41] It is even more influential overseas, holding 85 percent of the EU search engine market. Google Search advertising accounts for over one half of all Internet advertising revenue in the United States.[42] A 2010 study revealed that if Google were an Internet Service Provider, it would be the second largest in the entire world. Google's data centers consume around 1.5 percent of all electricity in the entire world. Google indexes 20 billion Web pages per day, handles of 3 billion daily search queries and offers free email to 425 million Gmail users.[43] In August 2013, between 50 and 70 percent of requests to Gmail, Youtube, Google Drive and Google's search engine went offline for one minute. As a result, global Internet traffic dropped by 40 percent.

Beginning as a search engine with the digital world's definitive web-crawling algorithm and extending into an empire that encompasses email, advertising platforms, a web browser and a social media network, albeit one that is less successful than Facebook, Google has managed to not only seep into almost every aspect of the typical American user's web experience, but streamline the process to consolidate all information into a

[41] Robert Waterman McChesney, *Digital Disconnect: How Capitalism Is Turning the Internet Against Democracy*. (The New Press. New York, 2013), 131.
[42] McChesney, *Digital Disconnect,* 143, 148.
[43] Powers, Shawn M., and Michael Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom*. (Chicago: U of Illinois, 2015), 89.

convenient, yet intrusive core that the company uses to maintain monetary and political power. Thus, a critical examination of digital advertising, privacy and policy in the U.S. is not complete without a look into a history of both the company itself, as well as the major mechanisms that define its digital advertising platform.

When Page and Brin began their conception of Google as a search engine, they developed the idea to use algorithms to simply figure out how to effectively and efficiently sort through sites on the Web. With the "dotcom bubble" hitting its apex, the two knew that the Internet industry was about to become extremely profitable. In 1998, they rejected the notion that their search engine would be supported by advertising. They were even quoted as saying: "We expect that advertising funded search engines will be inherently biased towards the advertisers and away from the needs of consumers. The better the search engine is, the fewer advertisements will be needed by the consumer to find what they want."[44]

The two developed PageRank, an algorithm that quickly made Google the best search engine on the web. The program is continuously being improved upon to this day. There is much more data on the web than search engines can interpret,[45] meaning Google's task was to figure out which specific data people wanted and needed to discover. While developing PageRank, the two learned more about search-engine bias within the fairly young industry. They discovered that advertisers were paying money to influence the results of a user's search query. This way, they could increase the likelihood that users would visit their site and subsequently purchase goods and services. Naturally the two found this process to be unethical and worse than advertising itself. "It is not clear who deserves to be there, and

[44] McChesney, *Digital Disconnect,* 101.
[45] Pariser, *The Filter Bubble,* 30.

who is willing to pay money to be listed," they reasoned. [46] Thus, their PageRank algorithm was based on scientific study and the organization of information independent of corporate support or money from advertisers.[47]

The PageRank algorithm was built to determine what publicly accessible Web content was closest to what a user was searching for when entering a particular term or query. The algorithm has grown to include more than just results themselves. It now can also return up to 29 special features to connect users with services quicker. These include synonyms, weather forecasts, time zones, stock quotes, maps, earthquake data, movie show times, airports, home listings and sports scores, to name a few. They now appear in a box at the top of the page.[48]

Brin and Page were as Eli Pariser described in his work, *The Filter Bubble*, "voracious" when it came to data collection and organization. "[They] were determined to keep everything: every Web page the search engine had ever landed on, every click every user ever made. Soon its servers contained a nearly real-time copy of most of the Web. By sifting through this data, they were certain they'd find more clues, more signals, that could be used to tweak results."[49] While these pursuits were done for the benefit of Google's developing algorithm, there is no doubt that this obsessive data collection was even then overwhelming and invasive. At the time, there was no need to share this information, but once the rest of the digital world got in the game and digital advertising took off, it was inevitable that data collection would become invaluable and essential to the success of other companies as well.

[46] Powers and Jablonski, *The Real Cyber War,* 87.

[47] Powers and Jablonski, *The Real Cyber War,* 87.

[48] Powers and Jablonski, *The Real Cyber War,* 88.

[49] Pariser, *The Filter Bubble,* 32.

PageRank worked successfully not by counting links from all pages equally, but rather by "normalizing by the number of links on a page… By taking into account the link structure among a network of pages, and employing a measurement based on the results, the structure of links was used in part to impose a structure of relevancy."[50] Google would reference pages that frequently came up as having appealing aspects to large numbers of previous users. Seth Finkelstein, programmer and winner of the Electronic Frontier Foundation's Pioneer award explained this in a more scientific manner:

> "PageRank relies on the uniquely democratic nature of the web by using its vast link structure as an indicator of an individual page's value. In essence, Google interprets a link from page A to page B as a vote, by page A, for page B. But, Google looks at more than the sheer volume of votes, or links a page receives; it also analyzes the page that casts the vote. Votes cast by pages that are themselves 'important' weigh more heavily and help to make other pages 'important.'"[51]

The data was not simply dumped onto a user's search results page. Rather there is post processing afterward that now involves customization depending on specific users.[52]

By 2000, Google had done a 180 and catapulted themselves into the growing world of digital advertising, launching their AdWords program in October of that year. AdWords is primarily an auction based pay-per-click ad service that allows any company or Web site to let Google place advertisements for their business on search result pages. The program

[50] Seth Finkelstein. "Google, Links, and Popularity versus Authority." In *The Hyperlinked Society: Questioning Connections in the Digital Age.* (Ann Arbor: U of Michigan, 2008), 104.
[51] Finkelstein, "Google, Links, and Popularity", 108.
[52] Finkelstein, "Google, Links, and Popularity", 109.

matches text ads to specific, relevant searches.[53] Where one's display is located (ie. how high on a page, what page), is based on an algorithm that combined things into a "quality score" that was derived from multiple factors including: relevance of keywords, monetary value of a keyword bid and click-through-rate – how often the displayed ad was clicked.

This new platform allowed advertisers the ability to match their products and advertisements to specific searches, meaning they could have a greater return on investment due to accurately targeted ads. It also allowed for each company to set its own specific maximum bid, giving companies room to compete to their own capacity.[54]While money is obviously a huge factor in success, there is an art involved as well. Companies and professionals who know what keywords to use and when, as well as what specific areas of the country and what demographics to target through IP address exclusion, have a greater shot at success. Google allows for these, along with a host of other customizable options. Many businesses now hire third-party digital advertising firms who excel at perfecting these campaigns along with search engine optimization (SEO). Because companies only have to pay Google when their ads are clicked on, a company theoretically will only be spending money when their ad is gaining traction, and thus, when they are making money. Hypothetically.

Over the summer, I started and ran an AdWords campaign for the company I was interning for. I knew nothing of the service or how it worked, and thus started very slow. I was given a budget of $10/day in spending, meaning that after clicks on my ad copy exceeded $10 in a day, my copy would no longer be displayed on search result pages. Cost-per-click is determined by certain keywords that users search. Certain popular keywords

[53] Powers and Jablonski, *The Real Cyber War,* 94.
[54] Powers and Jablonski, *The Real Cyber War,* 94.

are more competitive than others, and thus more expensive to bid on. For example, the average bid on the word "mortgage" was over $4, whereas the average bid for a phrase like "John Smith's real estate" might hover somewhere around $0.85 due to the fact that no one ever searched it. In reality, my cost alone made my quality score extremely low.

Knowing very little, I contacted what would at first be a complementary representative from Google who was instructed to help me with my campaign. Theoretically she would help streamline my keywords, reorganize my targeted demographics and geography and ultimately increase the effectiveness of my campaign. Over the phone, my guide explained things which she felt would be a good idea. Naturally my skepticism kicked in. Sure theoretically my success is Google's success, but why would a company want to help this genuinely. After I granted the Google employee access to the campaign, our click-through rate drastically improved. Yes we were spending more money, but for the first time in a few months, we were exceeding our $10 per day limit and chose to increase our budget. After a close look, I discovered that our clicks were all coming from our newly established mobile campaigns. The representative from Google had randomly placed our ads on things like online gambling pages, mobile games and other gimmicky platforms that were completely irrelevant to our demographic and our company's clientele. I quickly canceled the campaign and lowered the budget to redirect our efforts.

In 2012 Google had five billion ad impressions every day worldwide. This translated into more than $100 million per day in revenue from this program alone. In addition, Google made $50.5 billion in advertisement revenue alone in 2013.[55]

[55] Powers and Jablonski, *The Real Cyber War,* 94.

In 2003, Google launched AdSense, a program that allowed any company or web site to place ads automatically in designated places on their Web pages. These sites then become part of Google's Display Network, which scans each Web site to determine what types of ads would appeal most to particular users visiting each site. Campaigns can include text ads, image ads, mobile ads and video ads.[56] In 2010, Google began to refine this program by starting a user search history to match particular users to ads they might find appealing. AdSense collected $10 billion in revenue in 2011.[57] Naturally, Google's foray as a leader in digital advertising has not only paved the way for digital advertising trends, but is representative of the acceleration of the industry as a whole.

Google's other platforms, beginning in 2004 with Gmail, and continuing with various applications like Google+ were all designed to gather more complete and accurate data from every aspect of a user's life. If everyone is logged into all of Google's services and using a Google Chrome browser, every action they perform online will contribute to their Google digital profile. By 2008, Google had several patents for personalization algorithms as well.[58]In an idealized future for the company, the entire web will become a platform for Google. Eric Schmidt, Excecutive Chairman of the recently founded (2015) Alphabet Inc. parent company to Google, exclaimed, "The technology will be so good, it will be very hard for people to watch or consume something that has not in some sense been tailored for them."[59] This is something that deeply concerns Pariser. He notes: "As personalized filtering gets better and better, the amount of energy we'll have to devote to choosing what

[56] Powers and Jablonski, *The Real Cyber War,* 95.
[57] Powers and Jablonski, *The Real Cyber War,* 95.
[58] Pariser, *The Filter Bubble,* 34.
[59] Pariser, *The Filter Bubble,* 47.

we'd like to see will continue to decrease."[60] We will effectively be replacing curiosity with convenience. Pariser continues:

> "At the moment, we're trading a system with a defined and debated sense of its civic responsibilities and roles for one with no sense of ethics. The Big Board is tearing down the wall between editorial decision-making and the business side of the operation. While Google and others are beginning to grapple with the consequences, most personalized filters have no way of prioritizing what really matters but gets fewer clicks. And in the end, 'Give the people what they want' is a brittle and shallow civic philosophy."

Pariser even called Google's PR department and asked about their code of ethics that is used to determine what information is shown to whom. The public affairs manager stated that Google just wanted to give people the most relevant information, implying that there were no ethics involved. Google, along with other Big Data media giants like to resist the idea that their work has moral or political consequences.[61] In reality, Google is not only democratically redistributing knowledge, they are using this redistribution to create a system that accurately predicts people's tendencies and interests. This reorganization makes data easy to decipher and package as a commodity to their business partners. Because Google is so dominant, users are subliminally coerced into using its services, allowing its revenue to continue growing and it's data to become consistently more accurate.

[60] Pariser, *The Filter Bubble,* 69.

[61] Pariser, *The Filter Bubble,* 176-177.

Should the world be presented as it is or as it should be? Do algorithms manipulate what is real and what we want to see? How important is this distinction?[62] These are questions Seth Finkelstein believes are central to the way we conceptualize what Google is doing to the digital world. These “elite influencers” as Finkelstein describes them, have conflated popularity with authority. Links from popular sites carry more weight to a search engine. “The self-reinforcing nature of references within a small group can then be a very powerful tool excluding those outside the inner circle. Instead of democracy, there’s effectively oligarchy.”[63]

Google is collecting information from around the world, storing their data on expansive computer servers and interpreting said data to classify and analyze for relevance. This data is then transmitted to Google’s archive to Internet users through various services, where it is transformed into useable, helpful knowledge.[64] This is an idealistic view, however, it explains Google’s tremendous informational impact on the modern web. According to authors Shawn M. Powers and Michael Jablonski, Google’s ability to consolidate and classify the world’s information, making it accessible and useful is central to the company’s success and survival. Regardless, 97 percent of Google’s revenue comes from advertising.[65]

Today, Google knows everything about our identity, location and interests, simply, as they claim, to suggest additional information or activity it thinks you will enjoy. As Schmidt explained, “I actually think most people don’t want Google to answer their

[62] Finkelstein, “Google, Links, and Popularity”, 109.
[63] Finkelstein, “Google, Links, and Popularity”, 118.
[64] Powers and Jablonski, *The Real Cyber War,* 77.
[65] Powers and Jablonski, *The Real Cyber War,* 77-78.

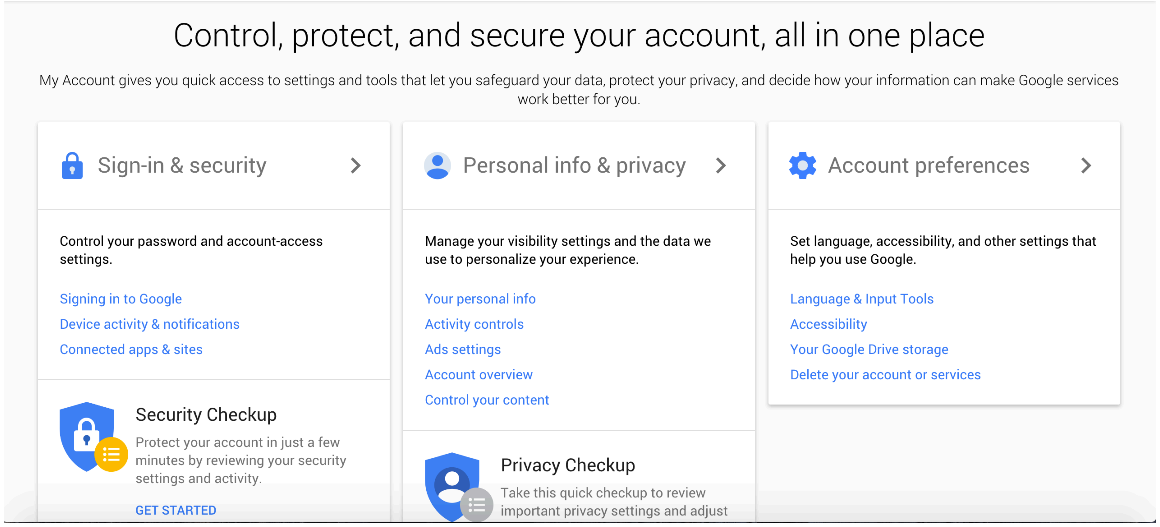
questions. They want Google to tell them what they should be doing next."[66]Google knows who we are, whom our friends are, where we want to go, and perhaps things that we could never even guess about ourselves. This alone is discomforting. When you pair this with the notion that Google's primary function is to match advertisers with the best chances of converting ads into sales, to match buyers to sellers, it gets downright unsettling. Our data, which now represents the every fiber of our digital being, is all that matters to a company whose primary goal is not to meet our needs, but rather those of advertisers. Google has been amassing this data for years. It has a detailed about practically everyone who has ever used the Internet. We don't search things, we Google them.

Google holds the key to our information, leaving us as helpless navigators in a world that unfolds itself according to our predetermined, yet evolving preferences. But what happens when this information gets in the wrong hands? Sure we surrender our privacy to this company, and sure our data is being sold at a rate we can barely imagine. But if nothing bad happens to us, as the majority of us can attest to, then who cares? The fear lies in the unknown. Powers and Jablonski wonder, "How vigorously does it protect user information from government and commercial investigators?" It doesn't just take a skeptic to note Google and Big Data's ties to the government at large. It is a reality of the modern age.[67]

As I was writing my chapter on the FTC, I went to do a Google search (I never said I was above the Internet Giant) and was prompted to switch the settings in my account to account for privacy. I *had* to click on the pop-up before I could access the Web again. I had never been prompted like this before. Was this a new feature, or was Google simply aware of my growing concerns for privacy and accommodating me accordingly? Was this Google's

[66] Powers and Jablonski, *The Real Cyber War,* 80.
[67] Powers and Jablonski, *The Real Cyber War,* 80.

way of appeasing me? Or was it an extension of their evolving, self-regulated privacy conditions?



Control, protect, and secure your account, all in one place

My Account gives you quick access to settings and tools that let you safeguard your data, protect your privacy, and decide how your information can make Google services work better for you.

Sign-in & security

Control your password and account-access settings.

Signing in to Google
Device activity & notifications
Connected apps & sites

Security Checkup

Protect your account in just a few minutes by reviewing your security settings and activity.

GET STARTED

Personal info & privacy

Manage your visibility settings and the data we use to personalize your experience.

Your personal info
Activity controls
Ads settings
Account overview
Control your content

Privacy Checkup

Take this quick checkup to review important privacy settings and adjust

Account preferences

Set language, accessibility, and other settings that help you use Google.

Language & Input Tools
Accessibility
Your Google Drive storage
Delete your account or services

Ironically, our best hope lies in capitalism. Companies like Google, Microsoft and Facebook have begun to compete on the quality of their privacy policies.[68] As I will examine in detail in the next chapter, the financial fates of all of America's Big Data giants are tied closely to the quality and adaptability of their privacy policies. Powers and Jablonski explain: "Google's fear of regulation of the Internet is genuine, as greater discretion regarding how governments control the flow of information within, into and outside its geographic space is of tremendous importance to the future of Google's business."[69] Luckily the U.S. government encourages self-regulation, allowing for companies like Google to work together with tremendous leeway to renegotiate their own privacy policies. There is no greater, single governmental body to which they must defer completely, no standard, user-centric policy that may curb their entrepreneurial endeavors.

[68] John G. Palrey and Urs Gasser. *Born Digital: Understanding the First Generation of Digital Natives.* (New York: Basic, 2008), 67.
[69] Powers and Jablonski, *The Real Cyber War,* 98.

CHAPTER 4: "BIG DATA" AND THE U.S. GOVERNMENT
Contemporary US capitalistic practices and the impact of public-private relationships on consumers' rights and privacy

How should the Internet be governed? What role does the United States government play in this process? Can we as a country govern "our Internet"? What role does the U.S.'s brand of capitalism play in the construction of the modern Web? The root to the answers of these questions lies in a close examination of modern American capitalism, along with 20th century events that shaped the binding relationship between government organizations and growing tech giants. As Robert McChesney stated in his work *Digital Disconnect*, capitalism and its relationship to democracy "should be the organizing principle for evaluating the digital revolution."[70] Through their ties to government entities, tech industry giants like Google, Apple and Facebook have aided the exponential acceleration of American capitalism to the extent that we run the risk of closing the gap between consumerism and culture in our society. Soon, we may live in a world where behavior is nothing more than a commodity, "a tiny piece of a market that provides a platform for the personalization of the whole Internet."[71]

> "Capitalism is a society where individuals freely come together in the marketplace to buy and sell products, including their labor. It is a free exchange; there is no coercion. Markets guarantee that supply and demand determine prices, which accurately reflect their products' value…Capitalism has always been incipient in humanity but it was only with the democratic revolutions that government was put in a cage and freedom and entrepreneurship flowered. This is the only democratic way to run an

[70] McChesney, *Digital Disconnect,* 13.

[71] Pariser, *The Filter Bubble,* 45.

> economy; any other system invariably involves the government or some other force, no matter how well intended, telling people and businesses what they should do, rather than letting people and businesses decide for themselves in the market."[72]

According to Professor Rob McChesney, author of the 2013 book *Digital Disconnect,* the recent high-tech revolution has created a new generation of what he calls "technophilanthropists" – giants in the tech industry a-la Mark Zuckerberg and Bill Gates – who are using their immense fortunes to appear to solve global problems. "These new emblems of capital are cool people, community minded and ecofriendly."[73] According to the aura these people propagate, the problems of the past will soon be solved by their innovative, world-saving technology and the uniting social power of their digital platforms. McChesney denounces this notion as "poppycock."

While McChesney admits that many of these technophilanthropists may have started with good intentions, the system of capitalism itself drove them towards a profit-oriented approach that now controls their means of survival as entities. "It is not that the managers are particularly bad and greedy people – indeed their individual moral makeup is mostly irrelevant – but rather that the system sharply rewards some types of behavior and penalizes other types of behavior so that people either get with the program and internalize the necessary values or they fail. Capitalism has an unforgiving logic: if you play, you have to play to win."[74]

[72] McChesney, *Digital Disconnect,* 23.
[73] McChesney, *Digital Disconnect,* 27.
[74] McChesney, *Digital Disconnect,* 28.

At the heart of this capitalistic-tech revolution is the proliferation of digital advertising. It is a major way to increase and protect market share without engaging in potentially profit-damaging price competition. As McChesney explains, "the more alike products are and the more similar the prices, the more the firms must advertise to convince people they are different."[75] Thus, the more firms advertise, the more stuffed with commercialism and advertisements certain aspects of our lives become. This begins to flood the media and our culture, meaning firms will have to advertise even more to stand out, and so on. Advertising soon begins to seep into new segments of society until it dominates virtually every aspect. New techniques in unique locations become "innovative" and capture the attention of those who may have previously become numb to ads in their typical venues. Advertising has become the dominant cultural force in the United States and is now, as McChesney dubs it, "the advance army of capitalism."[76]

Ironically, the Internet originally intended to completely eliminate advertising from our culture. In the 1960s and 1970s, computers were seen as anti-commercial as they represented values of egalitarianism and cooperation. In the 1970s, Steve Wozniak of Apple saw computers as "a tool that would lead to social justice." The democratic socialist government in Chile in the early 1970s devoted considerable resources to computing, believing it could provide efficient economics without the injustice and "irrationality" of capitalism. In the 1980s, computer professionals and students cultivated an open, non-hierarchical culture with few restrictions on how one could use the network. In 1993, *Advertising Age* claimed that the internet's culture "loathed advertising." Marketers and Madison Avenue were afraid that if they entered into digital advertising, they would be

[75] McChesney, *Digital Disconnect,* 42.
[76] McChesney, *Digital Disconnect,* 47.

greeted by "a tidal wave of flaming" from the digital community."[77] Companies could not figure out ways to effectively market their products to prospective consumers online. At first, people could actually escape from advertising all together on the web. So what happened?

The growth of patents became the first domino to fall in the now seemingly inevitable commercialization of the World Wide Web. One of the Internet's foremost expectations was that it would be open and free, a place to share for the common good. Still companies tried relentlessly to profit off of the then primitive medium of the Internet. Patents on certain technologies and sites began the slow process of establishing digital monopolies rather than incentives for research.[78]

In addition, the creation of cookies truly helped a revenue-based Internet take off conceptually. There was a need for a source of revenue for online content and services. A pay-per-view system was in itself unrealistic when put in the context of what old-generation Internet users believe in: a free, open source platform designed for an unrestricted flow of information. This was proven in practice. If sites attempted to sell access to their content, usage tracking quickly demonstrated that most Internet users would ignore those paid sites and move over to the rest of the seemingly infinite world of free content.[79]

By 1994, the privatization of the Internet began to take shape. There were no policies in place to determine what the Internet could or couldn't become. Corporations began to buy up sites and digital properties as they realized that they could have free reign

[77] McChesney, *Digital Disconnect,* 101.
[78] McChesney, *Digital Disconnect,* 103.
[79] McChesney, *Digital Disconnect,* 146.

over the growing medium. The earliest signs of government and corporate ties are now obvious in the 1996 Telecommunications Act. This act propagated that rising concerns with natural monopolies developing in the digital world were false, as the Internet had the power and intent to render them non-existent. This effectively meant there was no justification for digital regulation. McChesney explained, "The propaganda was so thick, no one stopped to ask why huge monopolistic firms would be lobbying for deregulation if it would leave them facing increased competition and therefore profits."[80] This act effectively served as a deregulation of the Internet. In reality these digital communication markets were all shaped and aided by the government based on existing government monopoly licenses and privileges.[81]

During the late 1990s, policies were created to promote the commercial development of the digital sphere. They made this commercial development appear to be beneficial and ingenious as they would inspire a "New Economy" rather than an elimination of advertising. This was spun into a positive, as policy makers claimed that this innovation would serve as "the solution to the growth problems of capitalism."[82] Before long, Internet heroes like Bill Gates emerged to represent the "positive" economic and social progress of the now bustling privatized, commercialized digital sphere.

But how were these government-corporate ties developed in the first place? The roots can be traced back to the Industrial Revolution. In order to cope with the seemingly overwhelming exponential proliferation of technology, Great Britain and the United states adopted a policy to restrict the outflow of information in order to protect economic

[80] McChesney, *Digital Disconnect,* 107.
[81] McChesney, *Digital Disconnect,* 107.
[82] McChesney, *Digital Disconnect,* 108.

advantages from technology that was invented or refined. This led to a contradictory way of viewing information in the U.S.'s perspective. Naturally, it should be freely available to all, yet access should be restricted so as to reward inventors and preserve the economic benefits of their inventions.[83]

Inevitably, the U.S. cultivated a close, codependent relationship with companies that were involved in the production, processing and distribution of information. When Franklin Delano Roosevelt passed the Social Security Act as part of the New Deal, providing American workers with long-term financial security during the Great Depression, the government realized it needed to keep track of salaries, wages and job records for millions of workers. It needed to monitor the fund and ensure proper distribution of resources once workers qualified for Social Security.[84] In other words, the government needed some sort of technology, like computers, to keep track of said information. It needed innovative minds to develop and facilitate this tech.

This relationship began to formally take form in the 1930s and 1940s. Modern information communications technologies were able to flourish through subsidizing policy reforms, direct investment and guidance as products like computers and the Internet were vital resources for the government itself. This eventually enabled the fruition and growth of Silicon Valley.[85]

Roosevelt turned to the now tech giant IBM in what was then considered the biggest accounting operation of all time. IBM was transformed from a struggling company to a

[83] Powers and Jablonski, *The Real Cyber War,* 27.
[84] Powers and Jablonski, *The Real Cyber War,* 53.
[85] Powers and Jablonski, *The Real Cyber War,* 51.

global tech and information leader.[86] Private-sector jobs now spurred innovation in infrastructure, technology and energy, all for the benefit of the government. This government-corporate relationship continued into the 1950s as the U.S. Department of Defense established the Advanced Research Projects Agency or ARPA in 1958. This was done to strive towards U.S. tech superiority in response to the Soviet's Sputnik satellite. Today, the organization, now called DARPA, with D standing for defense, still supports these types of endeavors.[87]

In January 1994, UCLA hosted the Superhighway Summit, the first public conference that brought together all industry, government and academic leaders. This conference served to further the public-private relationships between the government and private industries on a large scale. It featured speakers including Al Gore, the Vice-President at the time and the FCC chairman, alongside Walt Disney, Sony and Time Warner executives.[88]

The advent of 9/11 solidified the relationship further, this time based on a more urgent necessity. The Bush administration and governmental intelligence agencies like the NSA began reaching out to the private sector for accessing any and all communications that could be related to future attacks. The NSA pursued a "content-based, metadata approach to systematically collect and analyze communications with foreign actors and entities."[89]

Since the entire communications infrastructure in the U.S. is and was owned and operated by the private sector, this effort by the NSA called for a new, even more comprehensive public-private relationship. Telecommunications providers were asked to share call records and real time data. Although they tried to work within the parameters of

[86] Powers and Jablonski, *The Real Cyber War,* 53.
[87] Powers and Jablonski, *The Real Cyber War,* 55-56.
[88] Powers and Jablonski, *The Real Cyber War,* 60.
[89] Powers and Jablonski, *The Real Cyber War,* 69.

existing privacy laws, a technicality allowed for the private sector to cooperate completely, as the NSA's tone implied that the country's national security was at risk. These private corporations were told that they were solely responsible for helping to protect their country from future attacks.[90]

With these private resources, the NSA was able to easily track down the name, address and personal information of virtually every phone number ever dialed in the world. AT&T, Verizon and BellSouth, the three largest telecommunications companies at the time, all agreed to share their call data with the NSA.[91] Naturally, the bustling digital corporations in Silicon Valley followed suit. Today, Google is on the forefront of fighting a "cyber war". Many of their top employees have left their post for top positions in the U.S. government. For example, Policy expert Andrew McLaughlin left Google to serve as Deputy Chief Technology Officer for the Obama Administration.[92] In 2006 Google attempted to enter the Chinese market. By 2010, they noticed an complex and sophisticated attempt originating in China with the intent of hacking into their corporate infrastructure. This large-scale effort to access the secure information of their users, along with corporate information was just one of many efforts on the part of hackers to hack into numbers of major digital Western corporations. Naturally, Google turned to the NSA, strengthening their ties. They gave the governmental organization access to some of their data in order to better understand how the attack happened. They also provided them license to create

[90] Powers and Jablonski, *The Real Cyber War,* 70.
[91] Powers and Jablonski, *The Real Cyber War,* 71.
[92] Powers and Jablonski, *The Real Cyber War,* 75.

defense mechanisms to combat similar attacks in the future. Google *did* claim, however, that they would not divulge any of their users' privacy information.[93]

Google's lobbying expenditures in 2012 were the second largest of any corporation in the country. In 2014, they opened a new Washington D.C. branch office that is around the size of the White House. McChesney and others claim, "Data is the new oil," a resource that is potentially infinite yet still serves as a raw material for business; one almost on par with capital and labor.[94]

It is unclear just how much the government subsidizes the Internet, as it depends on how certain people analyze government spending itself. According to Sascha Meinrath:"It's fairly modest in terms of direct cash outlays. But once one takes into account rights of way access that were donated and the whole research agenda, it's pretty substantial."[95] When one includes things like wireless subsidies and tax breaks, it can range into the hundreds of billions range. According to McChesney, if one allows for inflation, a conservative take on Meinrath's estimate puts the investment at least ten times greater than the cost of the Manhattan project.[96] The following companies had these amounts in cash alone in 2012:

Apple	$110 billion
Microsoft	$51 billion
Google	$50 billion
Facebook	$16 billion

[93] Powers and Jablonski, *The Real Cyber War,* 184-185.
[94] Powers and Jablonski, *The Real Cyber War,* 75.
[95] McChesney, *Digital Disconnect,* 101.
[96] McChesney, *Digital Disconnect,* 101.

- Amazon - $10 billion[97]

These five companies, along with a small host of other "Big Data" giants, effectively hold a government-backed monopoly over the Internet. According to scholar Lori Andrews, "Facebook could not exist unless there were laws preventing it from being sued for invasion of privacy, defamation or criminal acts based on people's postings…Facebook holds the cards, and its citizens have little recourse – other than to leave the service entirely."[98] Luckily, as I will discuss further in a future chapter, the Federal Trade Commission encourages self-regulation, allowing Facebook and it's corporate buddies to determine their own privacy policies based on little more than a pamphlet of suggestions that is adaptable to what they find economically advantageous.

Facebook has also bolstered its lobbying team down in Washington DC, yet the spending of individual firms is merely a small part of the private tech industry's lobbying effort. Several governmental trade associations represent these "Big Data" giants, each with budgets in the tens of millions of dollars. They are so powerful, they are closing monetary the gap with Internet Service Providers and more traditional old media giants. For example, Mark Zuckerberg has been invited to the G8 meetings to discuss global politics, solidifying his place as a global leader. Because of the digital economy's fluid nature, these Internet firms can take advantage of the federal income tax code to move a large amount of their profits earned in the U.S. to accounts in foreign low-tax nations, dramatically reducing what they pay in taxes overall.

The privatization and commodification of the Internet succeeded due to both the rise of public-private ties based in government necessity, along with the elimination of

[97] McChesney, *Digital Disconnect,* 137.
[98] McChesney, *Digital Disconnect,* 142.

middlemen from a business perspective. On the surface, there was no “seller” on the Internet to interrupt the flow between what we wanted and how we consumed it. At the same time, the government desired to make the need for real, substantial information just enough of a nuisance for people to not bother looking critical information up. The personalization of the digital realm that we are now confronted with presents itself as a convenient solution, yet it simultaneously provides revenue for corporate companies who fulfill the government’s needs of concealing its information and obtaining ours. This age of “Post-materialism,” as Eli Pariser dubs it, allows for us to care about products and their idealized digital leaders because we don’t need to worry about our most basic needs being met.[99]

We as a country believe that we are creating our own world in the digital sphere. We believe that our desires are constructing this world without barriers, that this personalization will lead to healthier and happier lives. We passively acknowledge the commercialization of every aspect of our culture. Perhaps this is because it scares us. Perhaps we are truly distracted, hypnotized in every sensory aspect. Still, the government, with the aid of “Big Data” corporations, manipulates the truth through the curating, context and flow of information that we receive.[100] When Google is spending millions of dollars lobbying in Congress for a host of different provisions, how can we as citizens expect to believe that they have our interests above their corporate ones? These companies have a solidified relationship with government entities that dates back to the mid-20th century. It is engrained in the modern infrastructure of our country; this is how America operates. These ties run much deeper than citizens may expect. We are numbers, cogs in this

[99] Pariser, *The Filter Bubble,*157.
[100] Pariser, *The Filter Bubble,* 141.

machine that works interdependently with the government to play to its own interests. The digital identities we believe we create on our own volition are nothing more than compartmentalized pieces of data turned over by government-corporate alliances for profit and information.

CHAPTER 5: CURRENT LEGISLATION AND FUTURE IMPLICATIONS
The Federal Trade Commission, U.S. self-regulatory practices and implications of user-centric EU legislation

While corporate ties to the U.S. Government present a cynical view of the inner workings of digital advertising regulation and what becomes of our personal data, the U.S. does have a governmental body designed to guide these companies in their privacy practices. Unfortunately, these public-private ties seriously impact what amounts to little more than suggestive guidelines for how companies carry out their self-regulatory privacy legislation. Due to both these ties and weak, self-regulatory policy infrastructure, U.S. citizens are effectively at the mercy of illusive and convenient individualized privacy policies that do little more than further corporate interests while refraining from "inconveniencing" the citizens who must confront them.

In the United States, the Federal Trade Commission, or FTC, is responsible for the regulation of the content of digital advertising and disclosures made in privacy policies. While digital advertising is regulated by federal, state and municipal laws, the FTC is by in large, the only powerful, regulatory force dealing with these issues on the national level.[101] Although there is comprehensive legislation in place, the FTC's digital advertising platform is often vague, scattered and puts the onus of responsibility on the users themselves. Through their encouragement of self-regulation, the FTC has been able to effectively frame the U.S.'s conception of privacy and anonymity as one that is necessary for National Security and the further growth and innovation of the "Big Tech" companies with which it is so closely aligned.

[101] "Digital Advertising Regulation 101." (Interactive Advertising Beureau)
http://www.iab.com/digital-advertising-regulation-101/
Accessed 2 April, 2016.

While the FTC does do its best to protect the rights of users in the capacity in which it can, this interpretation of privacy does little, if nothing to curb the proliferation of digital advertising and personal data tracking. The United States government's business ties and monetary interests have disregarded the privacy rights of its citizens. The rest of the Western World is beginning to take notice. The European Union, a governmental body with a much more user-centric approach, has enacted much stricter data and privacy laws under the newly formed General Data Protection Regulation, or GDPR. As I discussed in the previous chapter, many U.S. Big Data giants like Apple and Microsoft rely on a tremendous percentage of their revenue to come from European countries. The U.S. and EU created the Safe Harbor agreement to ensure that companies can only trade oversees if their data meets the strict privacy standards set by the EU themselves. As recently as this past December, the U.S. was found to not meet those standards, and is thus in violation of the agreement. Ironically, the United States' company centric digital advertisement regulation platform may be its eventual undoing.

Through the course of this chapter, I hope to first give a critical interpretation of the FTC's policies, as well as a few examples of other regulatory forces on the federal and state levels. I will then take a look at the Safe Harbor agreement, the U.S.'s failure to comply and the stipulations of the new agreement reached this past February. Lastly, I will examine the EU's newly established General Data Protection Regulation to examine their different, user-focused approach to digital advertising regulation. While my thesis has taken a U.S. centric approach to digital advertising and privacy issues, the U.S. government's close ties to both domestic and European business makes a general understanding of EU regulation imperative.

The FTC and Hands-Off Data Regulation

According to Section 5 of the FTC Act: "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." This statement is both vague and malleable. The act goes on to clarify that advertisements causing economic injury could be considered "unfair." Yet rather than simply allow harmed users the opportunity to prove their economic injury, the legislation makes it so advertisers must substantiate claims with what the FTC can deem "competent and reliable evidence."[102] This may be required to include scientific data in certain circumstances, yet the implied certainty of scientific data is overstated.

Additionally, The FTC additionally provides guidance to help advertisers comply with the requirements of Section 5. Compliance with FTC law requires companies to make sure they are not misrepresenting, omitting or misleading consumers through their privacy policies. In 2013, it updated its "Dot Com Disclosures." These disclosures were initially released in 2000 to provide guidance as to how existing FTC regulation applied to the online sector. The updated accounted for the technological advances over the past 13 years.

This Dot Com Disclosures guide is to be viewed as a simple guideline for advertisers. It contains no definitive rules. Its primary purpose is to help companies avoid getting in trouble. One has to wonder why there is not a pamphlet like this for users. Many assume that the government will protect them; that there are laws in place to ensure their privacy. They just don't know what they are. This empty assumption, paired with the idea of self-regulation, a very American notion rooted in ideas of free enterprise and capitalism only further strengthen this wall between consumers and ad agencies. The FTC doesn't say why

[102] "Digital Advertising Regulation 101." http://www.iab.com/digital-advertising-regulation-101/ Accessed 2 Apr. 2016.

we should be concerned in its policy. Sure there is the argument that we cannot put this burden on the FTC. We should take action ourselves to help change the culture of the Internet. But is that really possible? This is the argument that Big Data and the government want us to have.

In 2010 the FTC encouraged advertisers to help users learn about behavioral tracking.[103] But that is the extent to which they pursued that problem. A mere suggestion, one that's implementation by these companies would do nothing but hurt their revenue. The Internet industry claims to think that the FTC overestimates these dangers, yet they say this again for their own interests. They attempt to shift the dialogue away from this discourse. Naturally everyone wants to satisfy advertisers. What we really need is a fundamental re-thinking of how we understand privacy and digital rights.

In addition, the FTC provides case highlights from previous consumer privacy consent orders so companies can better understand which online practices are deemed "acceptable." The FTC also recently published a guide for mobile app policy, including: telling the truth about what the app can do, disclosing key information clearly, building privacy considerations into the app from the start, offer easy to find and easy to use choices, honor privacy promises, protect children's privacy, collect sensitive information only with consent and keep user data secure.[104]

While this guidance is helpful and perhaps beneficial to both parties, its helpful nature towards businesses points towards a leniency that could allow for shortcuts, loopholes and an understanding of the system in place to the extent that companies can

[103] Turow, *The Daily You,* 180.
[104] "Digital Advertising Regulation 101." http://www.iab.com/digital-advertising-regulation-101/ Accessed 2 Apr. 2016.

achieve what they want in regards to data collection without breaking the law. While most site operators and app developers do now post privacy policies due to specific requirements to comply with scattered state laws and industry standards, there is no overarching federal law that requires website operators and app developers to have a privacy policy.[105]This is something I believe should be standardized throughout the domestic digital world. Compliance with privacy laws is also done to hold a position as "best in practice." In other words, a company with a good record in regards to its own privacy policy bolsters its reputation both among corporate entities and its own consumer base. This manipulation of policy manifested in self-regulation can be molded to serve whatever makes a company look best. This makes the incentive for user privacy rights primarily one for economic gain, a common theme.

The FTC's regulation puts a focus on practices that deceive customers, rather than the collection of Big Data itself. In addition, the FTC's penalties are often quite light for companies violating the law. While the Commission does often join with other law enforcement agencies to monitor the Internet for potentially false or deceptive advertising claims, fines reach up to the lowly sum of $16,000, a drop in the bucket for all Tech Giants in the U.S. This is not to say that the FTC hasn't worked to improve its policies and be more active in its protection of users.[106] A 2009 Staff report stated that they urged companies to:

- Explain the information they gather.
- Encourage firms to give audiences the choice of whether to receive targeted ads.

[105] "Retrospective Review of FTC Rules and Guides." *Federal Trade Commission.* N.p. n.d. Web. 22 Apr. 2016.

[106] "Digital Advertising Regulation 101." http://www.iab.com/digital-advertising-regulation-101/ Accessed 2 Apr. 2016.

- Inform consumers when privacy policies change and thus receive consent to use old data in new ways.
- Make sure data are secure and not retained indefinitely.
- Urge the use of 'sensitive data' about finance, health, sexual preferences to be "handled with great care to the point that consumers should consent, or affirmatively opt in, to their use."[107]

Still, the FTC must urge companies to commit to certain practices. Its power is cut off after it offers its suggestions. An analysis of this report by Joseph Turow in his 2013 work *The Daily You,* found this report to again support marketers needs rather than users' privacy. He went on to argue that the "FTC staff accepted that tracking and targeting had become part of the digital landscape."[108] Here, advertisers would not have to get permission to access data from users except in very sensitive cases. The U.S. also has no specific regulations requiring companies to explain why they collect and use data about individuals.[109]

While the FTC's regulation is vague and tends to support marketers' needs over users', some states have taken it upon themselves to provide additional regulation. One popular legislation focuses on requiring websites that collect or sell personal information of its residents to have publicly available privacy policies on their site.

The most prominent example of this is the California Online Privacy Protection Act of 2003 or CalOPPA. This legislation requires website operators and app developers to

[107] Turow, *The Daily You,* 174.
[108] Turow, *The Daily You,* 175.
[109] "Digital Advertising Regulation 101." http://www.iab.com/digital-advertising-regulation-101/ Accessed 2 Apr. 2016.

conspicuously post a privacy policy that “identifies the categories of personally identifiable information collected about the site visitors and the categories of third parties with whom the website operator or app developer may share the information.”[110] As of July 1, 2013, 46 states have laws on breach notification, 16 have laws addressing spyware and 15 have sectorial laws that address the collection and processing of financial, health and insurance information.[111] While some would consider this “a good start,” the reality of the situation is that the majority of states do not have sets of laws to protect them from these basic threats, let alone unified legislation. Should the Internet, a platform where state boundaries become moot, really be something that can and should be governed on a state-to-state basis?

To rationalize this lack of standardized legislation on the national level, the FTC and government encourage intense self-regulation. The Digital Advertising Alliance Self-Regulatory Program, or DAA, was formed as a result of the 2009 FTC staff report. Multiple organizations, including: The American Association of Advertising Agencies, the Association of National Advertisers, the American Advertising Federation, the Direct Marketing Association, the Interactive Advertising Bureau, the Better Business Bureau and the Network Advertising Initiativeformed together to create the DAA in 2011. A study conducted by Parks Associated found that only 6% of consumers were aware of the site in 2013. While this number jumped 21% to reach 37% awareness in 2015, it still has a long way to go to become a relevant and significant resource for users themselves.[112] The

[110] “Digital Advertising Regulation 101.” http://www.iab.com/digital-advertising-regulation-101/ Accessed 2 Apr. 2016.
[111] “Digital Advertising Regulation 101.” http://www.iab.com/digital-advertising-regulation-101/ Accessed 2 Apr. 2016.
[112] “AdChoices.” *Wikipedia.* Wikimedia Foundation. n.d. Web. 22 Apr. 2016.

program was designed to help protect consumers' ability to exercise notice and choice in ad-supported online media. They have the right to be notified of data collection and the choice to consent to its collection. The DAA currently issues Principles covering three distinct areas: behavioral advertising, collection and use of multi-site data, and the collection and use of mobile data.[113]

The DAA administers and enforces self-regulatory rules, which are in turn enforced by The Council of Better Business Bureaus and The Direct Marketing Association. If there is a possible violation by a member company that has partnered with the DAA, companies will work with the DAA to attempt to come into compliance with the self-regulatory stipulations. If the company still fails to cooperate, it faces possible suspension or expulsion from the membership.[114] Currently some of the largest corporations in the world, including Google, are members of the DAA. Still, if companies are given this leniency and a policy that allows for multiple strikes before expulsion, they are likely to take the policy itself less seriously. In addition, the partnership between companies and the DAA creates a strange grey area where "compromise" to come to a resolution could mean anything.

One of the areas with more extensive, protective legislation concerns the privacy of financial information. Both The Fair Credit Reporting Act (FCRA) and The Gramm-Leach-Bliley Act (GLBA) are in place to aid these efforts. The FCRA regulates the consumer reporting industry to establish privacy rights in consumer reports. The GLBA facilitates data sharing between financial institutions. Under the Act, institutions may share

[113] "Digital Advertising Regulation 101." http://www.iab.com/digital-advertising-regulation-101/ Accessed 2 Apr. 2016.

[114] "Digital Advertising Regulation 101." http://www.iab.com/digital-advertising-regulation-101/ Accessed 2 Apr. 2016.

information with affiliates as long as the customers are notified via general privacy policy. There is, however, no requirement for the customer to have the ability to opt-out. Financial institutions are also allowed to share information with non-affiliated companies. In order to do this, however, they *must* have the ability to opt out.[115]

Industry's progress throughout late 1990s and early 2000s hinted at more user-centric legislation. In a 1998 the FTC laid out principles for fair information practice. Later that year, they conducted a report that concluded that the vast majority of companies had not adopted even the most fundamental fair information practices.[116] The FTC held workshops in 1999 and 2000 where they released a report that recommended that Congress pass online privacy legislation as a basic level of data privacy protection.

In July 2000, they recommended that legislation be passed to protect Internet user's privacy in regards to online programing. Under this proposal, "all online advertising networks and consumer-oriented commercial websites that allowed the collection of information from or about consumers" would be required to comply with their previously mandated privacy principles, now called the Fair Information Practice Principles or FIPPs. Naturally, Congress did not enact the FTC's recommendation. By 2001, the FTC had begun to turn away from online privacy and develop its more hands-off approach. Then Commissioner Timothy Muris stated, "The slowing of the growth of the Internet emphasizes the need to understand the cost of online privacy legislation…At this time, we need more law enforcement, not laws."[117]This statement and sentiment served to change

[115] "Advertising and Marketing on the Internet: Rules of the Road." (*Federal Trade Commission,* Federal Trade Commission, Dec. 2000.) Accessed Web. 22 Apr. 2016.
[116] "Advertising and Marketing on the Internet" Accessed Web. 22 Apr. 2016.
[117] "Advertising and Marketing on the Internet" Accessed Web. 22 Apr. 2016.

the direction of where the FTC, and America in general's perceptions of privacy, big data and user protection would head in the future.

Authors John Palfrey and Urs Gasser agree with the second part of Muris's statement in their 2008 work *Born Digital: Understanding the First Generation of Digital Natives*. They observe that the FTC is constantly understaffed and underfunded when it comes to its enforcement efforts. They also recommend changes to the legislation that could help streamline the process and make enforcement easier. They conclude: "Law could mandate clear, simple labeling of privacy policies. The state mandates that certain consumer food products have a standard label to list the nutritional facts about the food. In the same manner, the state could make it easier for Digital Natives and others to manage their online identities by mandating that Web services provide clear, standardized labeling for their privacy policies." Suggestions include a new, icon-based system that could show how long data is stored before it is deleted.[118]

Palfrey and Gasser mention what the idea of technological determinism, as coined by Thorstein Veblen, assuming that society's technology drives the development of its social structure and cultural values.[119] In this vain, they point out what Muris argued back in 2001, that badly designed and overarching privacy legislation could hamper innovation and that privacy protections could make it tougher for law-enforcement personnel to do their jobs tracking down criminals.[120] There is a notion that Americans trust companies more than they trust their governments, an adage that works the other way around in Europe. Palfrey and Gasser observe: "Laws should let users decide what happens to data

[118] Palfrey and Gasser, *Born Digital,* 74.

[119] "Technological Determinism." *Wikipedia.* (Wikipedia, 20 Mar. 2016.) Accessed 1 Apr. 2016.

[120] Palfrey and Gasser, *Born Digital,* 77.

about them, not the corporations that collect the data." They reference European Style Laws, explaining: "They put the individual in control of his or her personal data. This is less popular among lawyers in the US but has recently received much attention among scientists and US tech firms that work on better ways to protect online privacy. [There is a] shift toward user-centric privacy controls while providing adequate support to users in their efforts to maintain these controls." In addition, the law should focus on a regime that protects consumers from data breaches. Companies that store information about users should be held to a responsible standard for maintaining their data collection's security.[121]

Robert McChesney comments on the reality of legislation like this getting passed in his 2013 work *Digital Disconnect*. McChesney concludes:

> "There is little evidence at this writing that the FTC or Congress will get much more aggressive, in large part because of the political power of the Internet giants, which desperately need to expand their data collection to make profits. Even under the glare of attention in Europe in 2012, and knowing it would generate criticism, Google instituted a new privacy policy by which it consolidates all the data from 60 different Google activities into a single database."

This highlights the insistence of the FTC and government at large on self-regulatory initiatives as the best solution. Companies will create their own "privacy policies" to comply these regulations and save face. Yet in reality, these policies can contain almost anything – the only thing that matters is the idea of a policy coming into fruition. Its

[121] Palfrey and Gasser, *Born Digital,* 79.

stipulations are largely ignored and favor the companies' interests. A look into recent developments between the US and Europe seriously challenges this notion.

EU Regulation and The Safe Harbor Agreement

On October 6, 2015, a ruling by the Court Justice of the European Union invalidated the United States-European Union Safe Harbor framework, sending shockwaves through the U.S. and EU business communities. Under the Safe Harbor agreement, U.S. companies need to self-certify to the U.S. Department of Commerce that they comply with specified EU privacy standards. Under the EU Data Protection Directive, personal information about EU citizens can only be transferred from the EU to countries with "adequate" data protection. Only a small handful of countries satisfy this requirement. The United States is not one of them. Therefore, the European Commission provided several ways for companies not in those countries to conduct such transfers. The Safe Harbor agreement was negotiated between the U.S. Department of Commerce and the European Commission back in 2000 to do just that.[122]

Because both the U.S. and EU rely so heavily on the transferring of data, failure to reach an agreement could severely damage the industries both here and abroad. In Skadden Arps' Intellectual Property Law Privacy and Cybersecurity Update this past October, the firm discussed the implications of this ruling. The decision highlights two key issues:

[122] "Skadden Arps. Privacy and Security Update October 2015." (*Privacy and Security Update (2015):* 1-8. *Skadden.com.* Skadden Arps. Oct. 2015.) Accessed Nov. 2015.

- We have entered a new era in which EU privacy rights could have a direct and significant impact on commerce between the EU and US. This Comes at a time with concerns within the business community that the EU data protection law – the General Data Protection Regulation – will impose new and significant obligations on companies that handle any EU personal data, with potentially large sanctions for failing to comply.
- Access by the US government to personal information for intelligence purposes is having an impact on the country's commercial uses of data.

Corporate ties in the US could make the process of negotiating a new agreement more lenient as the government has economic incentive to allow company access to the Safe Harbor agreement. As of 2015, over 4,500 U.S. companies had joined the Safe Harbor. According to the *Schrems* court decision, the Court of Justice found that the Safe Harbor was invalid since it does not address the U.S. government's nearly unrestricted access to much of its data. It also found that, despite the fact that the European Commission determined that the Safe Harbor provided an adequate level of protection for data, "individual data protection commissioners in the EU member states have 'complete independence' to conduct their own investigations and make their own determinations of adequacy, and are free to challenge the European Commission's decisions before the Court of Justice."[123] Thus

[123] "Skadden Arps. Privacy and Security Update October 2015." (*Privacy and Security Update (2015):* 1-8. *Skadden.com.* Skadden Arps. Oct. 2015.) Accessed Nov. 2015.

despite their strict regulation, the reality of the situation is that EU companies have just about as much free reign as they want as well.

In this interim period, the U.S. *did* actually have several limited options to comply with EU law. They could either obtain expressed consent from data subjects themselves, though this consent could be revoked or they could enter into "model contracts" based on agreements approved by the European Commission. In addition, if both transferor and transferee were part of the same multinational corporation, they could adopt binding corporate rules approved by local data protection authorities, though this could take over 18 months.[124]

There are also a number of other countries that have data protection laws similar to the EU and are thus following the EU's lead on determining whether certain countries' data protection laws are adequate enough to permit transfer. A good example of this is Israel. Isael passed the Israeli Law on October 19, 2015. The Information and Technology Authority announced it was revoking its approval of data transfers to the U.S. that were based on the Safe Harbor.[125]

The EU published a list of 13 recommendations to revise the Safe Harbor for greater protection of personal data. Many of these stemmed from the Snowden discoveries. In 2014, the EU and U.S. entered negotiations for a new Safe Harbor agreement. However, the *Schrems* court decision made it so national data protection authorities would retain the

[124] "Skadden Arps. Privacy and Security Update October 2015." (*Privacy and Security Update (2015):* 1-8. *Skadden.com.* Skadden Arps. Oct. 2015.) Accessed Nov. 2015.

[125] "Skadden Arps. Privacy and Security Update October 2015." (*Privacy and Security Update (2015):* 1-8. *Skadden.com.* Skadden Arps. Oct. 2015.) Accessed Nov. 2015.

power to review data protection practices, and subsequently make authoritative decisions on their own. A three-month grace period was given in October to negotiate an agreement. Until then, EU data protection regulators would have to refrain from taking action against companies using other means to address these concerns.[126]

While the January 31, 2016 deadline passed without an agreement, the two sides reached a deal two days later. The Safe Harbor agreement was replaced with the EU-U.S. Privacy Shield. If this is approved, it will provide a new framework under which U.S. companies can transfer personal data from the EU to the U.S. under the EU Data Directive. The specifics of this agreement have not yet been revealed, as the agreement must be approved from both sides. It looks to provide more lenient regulation according to Skadden's speculation: "Overall, the agreement seeks to balance the fundamental right of privacy of EU residents with the needs of the U.S. intelligence committee while also creating a workable system for U.S. companies." The agreement should take several months to be finalized.[127] Unfortunately, this "compromise" sheds a much more optimistic light for U.S. and EU corporate entities than for users' privacy rights. After all the deal was done by the U.S. (and presumably in the interest of EU corporations) to resume trade above secure the rights of U.S. citizens.

In addition to the Safe Harbor agreement and subsequent compromise with the U.S., the EU has been working on its own updated data protection legislation. The General Data

[126]"Skadden Arps. Privacy and Security Update October 2015." (*Privacy and Security Update (2015):* 1-8. *Skadden.com.* Skadden Arps. Oct. 2015.) Accessed Nov. 2015.

[127] "Skadden Arps. Privacy and Security Update October 2015." (*Privacy and Security Update Historic New Privacy Shield Agreement Replaces EU US Safe Harbor:* 1-8. *Skadden.com.* Skadden Arps. Jan. 2015.) Accessed Feb. 2016.

Protection Regulation, or GDPR, was negotiated this past December and will likely go into effect in two years. There is intense backlash from European business that Skadden believes will likely continue despite the approval of the bill. The regulation will apply to all member states, although it has a number of provisions that permit "customization," effectively making the law feel like several scattered laws throughout Europe.[128]

The GDPR applies to both data controllers and processors in the EU, as well as those outside the EU that's services offer good to EU data subjects. It eliminates the uncertainty of what constitutes "personal data" that was often disputed over the previous Directive enacted in 1995. It also speaks specifically to concepts of "anonymized" data, which will now be treated the same as personal information and accounts for stricter profiling regulation as well. Fines for breaching the GDPR could result in fines of up to 20 million Euros, a much heftier fee than the $16,000 instituted by the FTC**.**

Common thought is that this tighter, user-centric regulation could help put US corporations more in line with users' rights. Still, deep down these entities must be concerned with themselves and their monetary worth. The EU holds a stronger government presence, but even if this becomes true in the U.S., how will existing corporate ties impact newer legislation? Privacy policies can be tools for companies to better their reputations and comply with "suggestions" put forth by the government, rather than operate for the benefit of the people who, according to certain perceptions on both sides, perceive them to be nothing more than a nuisance. In addition, do these differing ideologies

[128]"Skadden Arps. Privacy and Security Update December 2015." (*Privacy and Security Update (2015):* 1-8. *Skadden.com.* Skadden Arps. Feb. 2015.) Accessed Feb. 2016.

between the two governments truly reflect a difference in ideology between the people, and more importantly, between U.S. and EU corporations?

Ironically, the fate of digital advertising and privacy regulation in the United States will almost inevitably be defined by government-corporate monetary interests. While populist movements pushing for digital privacy and centralized regulation are plausible, the cynic in me finds them a bit idealistic. Rather, the U.S.'s net worth and stock are a more realistic and important reason for them to take action. Even if they do, will the newer, centralized laws privilege the rights of users over those of companies who yearn to make a few more bucks?

CHAPTER 6: THE PEOPLE AND PEW
Assessing discontent and apathy in U.S. citizens in an age of corporate dominance and rapid technological advancement

Throughout the course of my work, I have closely examined the ways in which our digital lives are impacted by "Big Data" digital advertising corporations and tech giants who commodify our self worth online. Through an examination of the history of the western world advertising industry itself, modern "Big Data" tech giants through the lens of Google and a close look at the evolution of American capitalism that facilitates public-private ties between the government and corporations and their implications on U.S. digital advertising and privacy policy, I have been able to begin to explain how we've gotten to where we are, and why policy exists the way it does. Still, equally important in this equation is the people's perceptions of the forces that impact them. How much do they know? How much do they care? Who knows what matters to those living in this digital generation prove telling of modern policies' implementations and could signal how future regulation may be mapped.

As Palfrey and Gasser put it, "Most young people are extremely likely to leave something behind in cyberspace that will become a lot like a tattoo – something connected to them that they cannot get rid of later in life, even if they want to, without a great deal of difficulty."[129] They argue that avoiding the Internet and these digital publics is not a solution and instead advocated for newer, more nuanced ways to navigate them. They acknowledge that society needs to start taking these privacy concerns more seriously as they are extremely unlikely to just "go away." They put the onus on parents, teachers and policymakers alike, noting that no one from this digital generation has lived through

[129] Palfrey and Gasser, *Born Digital,* 53.

adulthood and experienced the effects of years of corporations having records of their compounded data.[130]

The authors highlight a gap in digital literacy and participation, urging adults to teach their children and the younger generation as a whole how to effectively operate and navigate the digital sphere. Yet is this enough? Sure our generation has lost control of the information we share online (whether it be voluntary or involuntary). But how will digital awareness alone be able to combat these corporate and government entities. Palfrey and Gasser claim that the most promising solutions are to emphasize peer-based learning and activism.[131] But in a society where consumer culture is the dominant culture and is transitioning into the only form of culture, we surely need larger forces to cooperate as well. The authors note: "The paradigm needs to switch from a firm-centric model, where companies choose what to do with user data, to a user-centric model in which ordinary people, not just the most tech-savvy, can manage themselves."[132]

As I discussed in earlier chapters, the advances of technology in conjunction with the growing corporatization of the Internet have led to a platform where trivial amusements compete for our attention. Perhaps this has created a certain segment of ultra savvy users and consumers who are not only aware of what is happening to their data, but are adept at navigating the web on their own terms. The problem here is, as Stacey Lynn

[130] Palfrey and Gasser, *Born Digital,* 55, 58, 62.
[131] Palfrey and Gasser, *Born Digital,* 69.
[132] Palfrey and Gasser, *Born Digital,* 73.

Schulman writes, "[Consumers] will gladly give up privacy for convenience and personalization. The slippery slope is to know when and where the line is."[133]

Perhaps the most accurate research done on the modern public's sentiment regarding digital advertising and privacy has been conducted by The Pew Research Center, a non-partisan American think tank based in Washington, D.C. that provides information on social issues and public opinion in areas like U.S. Politics and Policy, Journalism and the Media, Social and Democratic Trends and the Internet, Science and Technology. Pew began research on a project they dubbed, "The State of Privacy in America: What We Learned" in June 2013 after the leaks by Edward Snowden. After a two and a half year effort, they were able to put together a comprehensive report of how people viewed government surveillance, as well as commercial transactions that involve the capture of personal information.[134]

The report began with a depressing, yet predictable statistic: 91 percent of adults agree or strongly agree that consumers have lost control of how their personal information is used and stored by companies. Half of these users said that they are worried about the amount of information about themselves that is available to companies online. In addition 88 percent of adults agree or strongly agree that it would be extremely difficult to remove inaccurate information about them from the digital sphere. 80 percent of those who use social networking sites are worried about third party advertisers and companies accessing

[133] Stacey Lynn Schulman, "Hyperlinks and Marketing Insight." In *The Hyperlinked Society: Questioning Connections in the Digital Age.* By Joseph Turow and Lokman Tsui. (Ann Arbor: U of Michigan, 2008), 145-158.
146

[134] Lee Rainie, "The State of Privacy in America: What We Learned." *Pew Research Center RSS. (*Pew Research Center, 20 Jan. 2016.) Accessed Feb. 2016.

the data that they share on said sites. 70 percent of users are worried about the government doing the same without their knowledge. Only nine percent of users feel they have "a lot" of control over how much information is collected about them and how it is used.[135]

This information sheds light on the sentiments of digital users throughout the country, showing that not only are they aware of what corporations and the government are doing, they have also, by in large, given up hope in keeping their information private. The study states, "Experts argued that privacy was no longer a condition of American life. It was rather a commodity to be purchased."[136] Americans also expressed a consistent lack of confidence about the security of their every day digital communication channels, having a lack of faith in both public and private organizations. Only six percent of adults expressed that they were "very confident" that government agencies would keep their records private and secure. 25 percent said they were "somewhat confident." On the flip side, 76 percent of adults said that they were "not too confident" or "not at all confident" that records of their activity maintained by online advertisers who placed ads on sites they visit would remain private and secure. 69 percent and 66 percent felt the same way about social media sites and search engine providers respectively.[137]

The study concluded that most Americans, rather than simply looking to protect their privacy, weigh a "digital era trade-off" with factors like terms of deals, circumstances

[135] Rainie, "The State of Privacy in America: What We Learned." *Pew Research Center RSS. (*Pew Research Center, 20 Jan. 2016.) Accessed Feb. 2016.
[136] Rainie, "The State of Privacy in America: What We Learned." *Pew Research Center RSS. (*Pew Research Center, 20 Jan. 2016.) Accessed Feb. 2016.
[137] Rainie, "The State of Privacy in America: What We Learned." *Pew Research Center RSS. (*Pew Research Center, 20 Jan. 2016.) Accessed Feb. 2016.

of their lives, whether they consider certain companies involved to be trustworthy, what happens to their data after it is collected and how long it will be retained.[138] In essence, they have defaulted to nothing more than a compromise; a loss of faith and hope in the process that would retain their privacy. This highlights the further acceleration of the consumer culture state, one that will soon allow for no wiggle room outside of the commercial sphere.

On the flip side, 74 percent of users consider it "very important" that they are in control of who can obtain information about them and 65 percent consider it "very important" that they control what information is collected. Still the survey indicates that they understand that the realities of the digital age mean they won't be able to be "left alone" and untracked. Still they want to have a say. In conjunction with this, 86 percent of users have taken steps to either remove or mask their digital footprints. Yet many say they are unaware of potential tools they could use and would do more if they had the know how.[139] Users want to have more control, they just don't have the knowledge to implement their desires. This highlights the gap in digital knowledge and discourse that Palfrey and Gasser discussed.

Unsurprisingly, a majority of the U.S. public believes that changes in the law could make a difference in protecting their privacy, specifically when it comes to the retention of their data. 68 percent of Internet users believe current laws are not good enough to protect people's privacy online. 64 percent believe the government should do more to regulate

[138] Rainie, "The State of Privacy in America: What We Learned." *Pew Research Center RSS. (*Pew Research Center, 20 Jan. 2016.) Accessed Feb. 2016.
[139] Rainie, "The State of Privacy in America: What We Learned." *Pew Research Center RSS. (*Pew Research Center, 20 Jan. 2016.) Accessed Feb. 2016.

advertisers, specifically in the way they handle personal information.[140] Savvy users themselves acknowledge that the onus is on the government here. That these corporate ties do nothing but allow for increasing corporatization of the digital world and the proliferation of consumer culture through the masking of self-regulation. The final conclusion of the survey reveals a dark prediction: That few individuals will have the resources to protect themselves from "dataveillance in the coming years. Even more horrific, data experts predict: "The prospect of achieving bygone notions of privacy will become more remote as the Internet of Things takes hold and people's homes, workplaces and the objects around them will "tattle" on them."[141]

Robert McChesney acknowledges the worst of these fears to the extent that he calls for the abolishment of capitalism in the conclusion of his work. While I will not go quite that far, I acknowledge that the points McChesney and others raise mirror the sentiments of the country, the track record of public-private relationships and the future of privacy and consumer culture in America. McChesney notes that the system appears safe from political challenge for now.[142] While this may not be true, a cynical, yet accurate perspective sees that change will not come from the people, whose voices are finally being heard. Nor will it come from a government who recognizes what is wrong with existing legislation. If it happens at all, it will instead come out of global business interests that force the U.S. regulation to comply with stricter, centralized regulation throughout the rest of the Western business world.

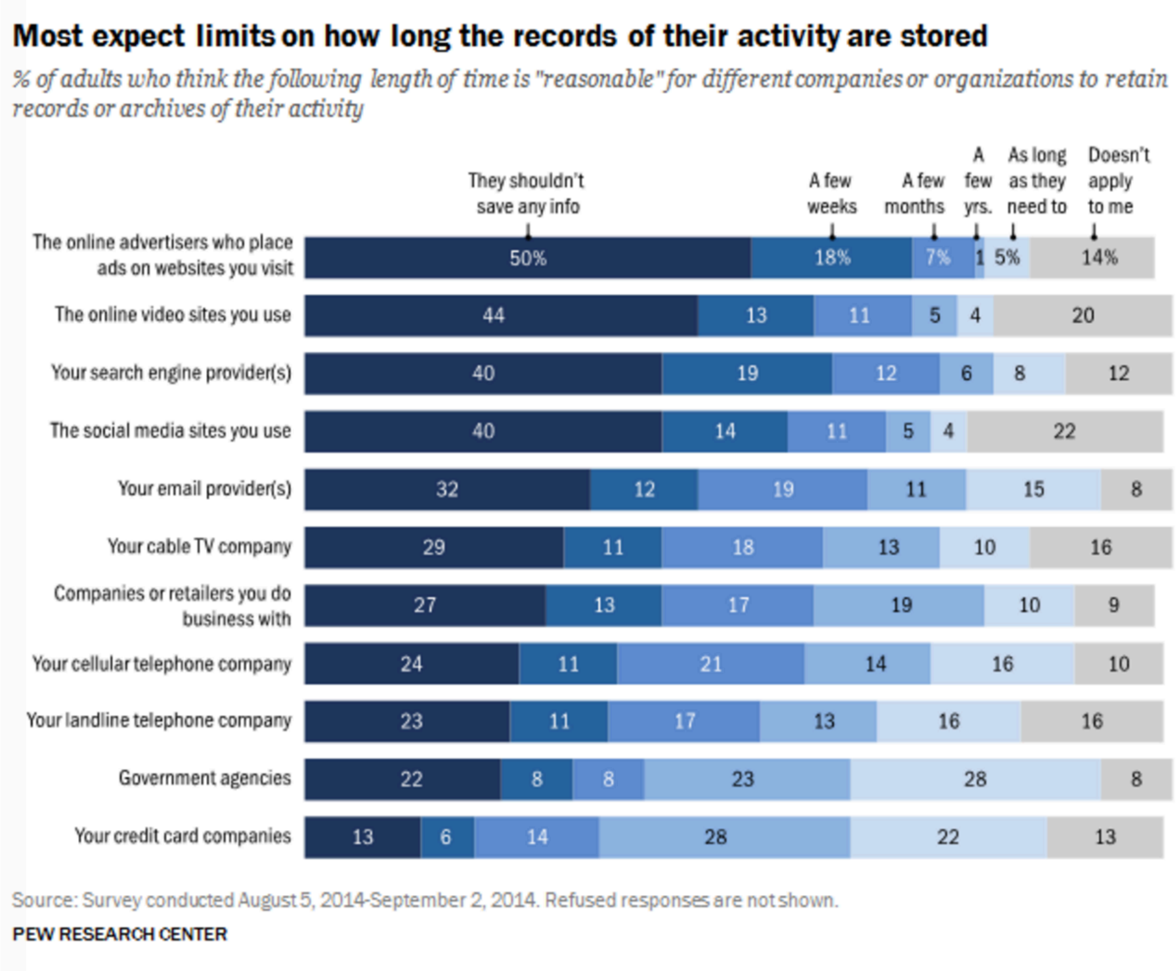
[140] Rainie, "The State of Privacy in America: What We Learned." *Pew Research Center RSS. (*Pew Research Center, 20 Jan. 2016.) Accessed Feb. 2016.

[141] Rainie, "The State of Privacy in America: What We Learned." *Pew Research Center RSS. (*Pew Research Center, 20 Jan. 2016.) Accessed Feb. 2016.

[142] McChesney, *Digital Disconnect,* 152.

We can enact as many digital literacy practices as we want. Yet with this accelerating rate of new technology and digital practices, we may already be a generation too late. Americans' conceptions of privacy and their overall lack of faith in the system show an slightly unknowledgeable, yet totally defeated public. Education is vital to growth and development, yet it must come from the top down along with grass roots efforts. In essence a broader political revolution is necessary to create real tangible change without influence from domestic and global business entities.

ADDITIONAL PEW DATA:



Most expect limits on how long the records of their activity are stored

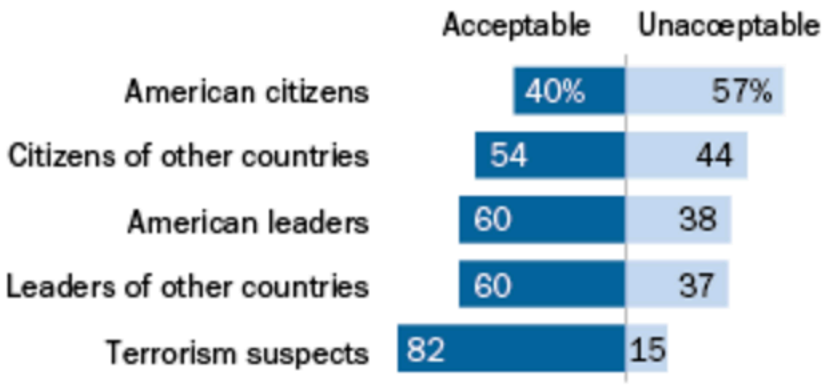
% of adults who think the following length of time is "reasonable" for different companies or organizations to retain records or archives of their activity

Source: Survey conducted August 5, 2014-September 2, 2014. Refused responses are not shown.

PEW RESEARCH CENTER

Most Americans believe it is acceptable to monitor others, except U.S. citizens

% of U.S. adults who say it is acceptable or unacceptable for the American government to monitor communications from ...

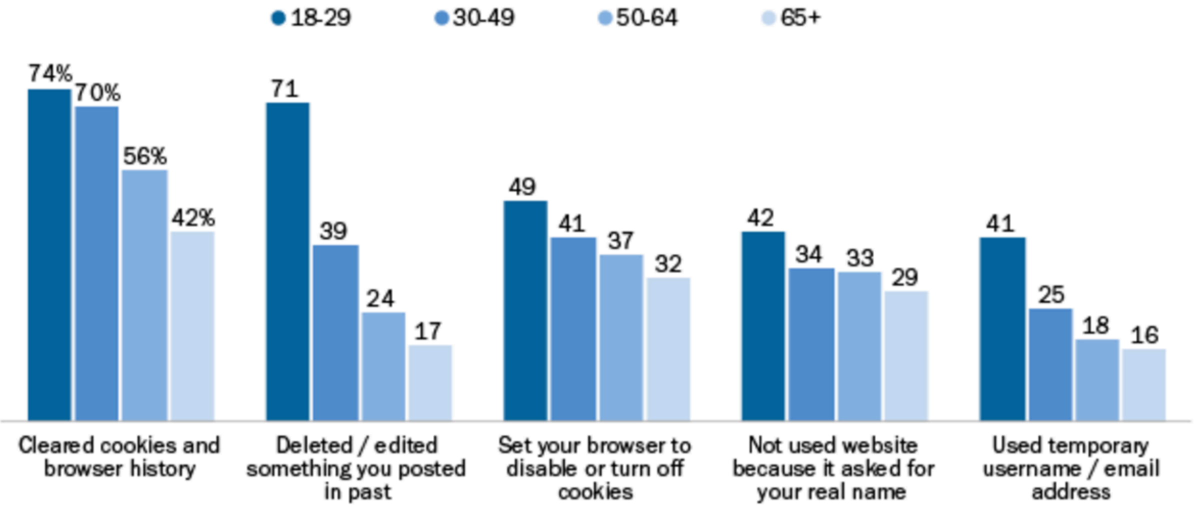


Source: Survey conducted Nov. 26, 2014-Jan. 3, 2015.

PEW RESEARCH CENTER

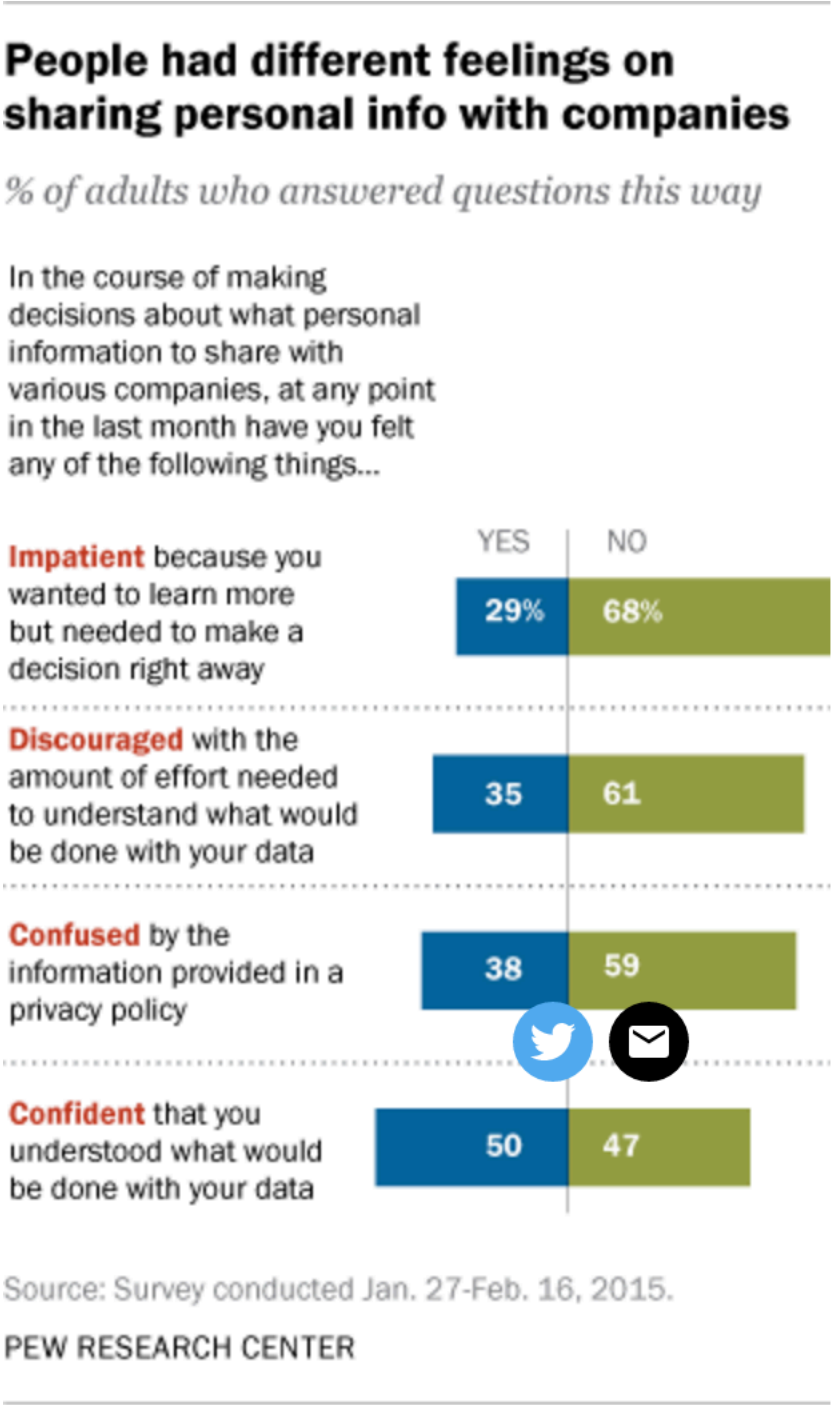
Young adults are the most likely to use most strategies to be less visible online

% of adults who report varying levels of sensitivity about the following kinds of info



Source: Survey of U.S. adults conducted Jan. 10-27, 2014.

PEW RESEARCH CENTER



People had different feelings on sharing personal info with companies

% of adults who answered questions this way

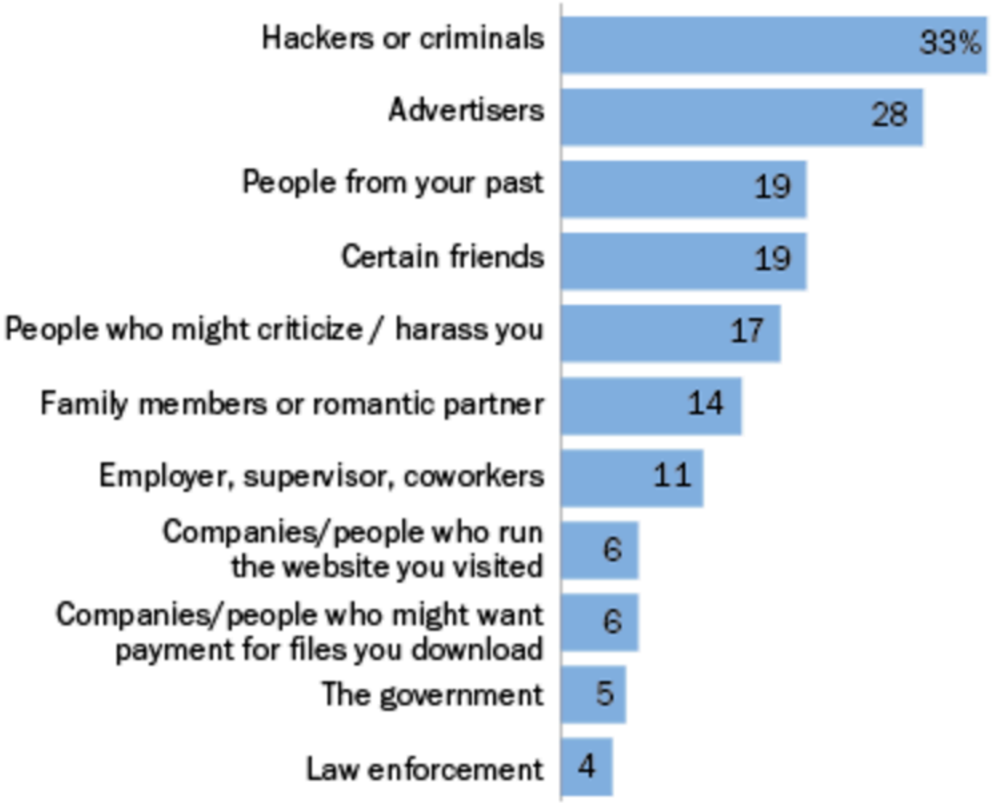
In the course of making decisions about what personal information to share with various companies, at any point in the last month have you felt any of the following things...

Source: Survey conducted Jan. 27-Feb. 16, 2015.

PEW RESEARCH CENTER

Who users try to avoid

% of adult internet users who say they have used the internet in ways to avoid being observed or seen by …



Source: Survey conducted July 11-14, 2013.

PEW RESEARCH CENTER

CHAPTER 7: CONCLUSION

> “The reason is the corruption of the policy-making process. In really existing capitalism, the kind Americans actually experience, wealthy individuals and large corporations have immense political power that undermines the principles of democracy. Nowhere is this truer than in communication policy making. Most Americans have no idea that debates on policy could even exist or what the actual deliberations are, due to an effective news blackout on the topics, except on occasion in the business press.” – Robert McChesney, *Digital Disconnect*

Personalization feels good. It is soothing, easy, as if someone is there tending to your every need. Through your actions and navigation, you are creating *your* Internet. But that misinterprets the Internet’s true purpose and value. We need a standard Net, not personalized browsers, pages, sites, etc. that systematically socialize people into different groups based upon preferences. The indirect consequences of digital advertising and marketing exploit users for profit, yet they also work to categorize them, limiting their access to knowledge. The products users see translate to the digital class they are put in based on things like income, credit score, geographical location, home, amenities, and even unclear things like what products they search for and what brands they enjoy.

Even if the direct, explicit motivation is to make money, the categorization is dangerous and inherently related to Web navigation, information retrieval, and a manipulation not just of how people navigate the online world, but the type of content they *learn* to search for and how they perceive the Internet in general. Someone who wants to seek out information will initially be rewarded by having an information dominant web experience, but those who search for products, entertainment, “cheap” or “shallow” content, and want the latter, even if only on occasion, will be subjected to a personalized experience that values that experience over all others. Hypothetically, a web experience that values any one thing over another for a particular user based on their past experience runs the risk of destroying the idealized, democratic message of what the Internet is and was meant to represent.

Obviously most of this is speculation into a future where today’s practices are accelerated and improved upon. Yet even if services theoretically become “perfect” in their predictions, in their recommendations and personalizations, they will have changed the message of what the Internet claimed to, and what I feel it should, represent. The Internet *should* be neutral. It *should* be the same for everybody. Everyone should be able to access what they want, but do so the same way, so as to ensure democracy and anonymity that protects their right to learn, their right to discover, and their right to share the same way it affects every other living person.

It boils down to access of information. If I can go to the library, I should be able to see all the books out in the open. Even if I’m looking for books on cooking, I should have to walk to the cooking section in the basement. If my friend comes in but wants to find comics, he should have to walk to that section and get them. Sure, it would be convenient if I came in and the cooking section of the library was placed in the main lobby for my advantage. The same would be true in the case of comics for my friend. Yet the accelerated technology and processes of the future Internet in this analogy would theoretically obscure the rest of the library and its catalogue, giving me what I want when I want it, but in its assumption, limit my access to the rest of the catalogue. People must get past their “I want it now right in my face at this instant" urges to protect their equal opportunities. This only supports a further fragmentation and specialization of society.

The Pew Research Polls indicate that people have given up, that they don't care. Users acknowledge that this is bad but also acknowledge that there is nothing they can do about it. With no overt, damaging repercussions, they will continue to demonstrate apathy. It's not about what is or isn't happening now, but the accelerated process that has the potential to completely change the fabric of our future society. All of these people who say that we need to individually learn, individually be educated - guess what? Companies know this. They know how to subvert our minds. They will make this education moot.

Sure a small percentage of people will go through the channels to access the web anonymously. Yet they do so in exchange for Internet speed, flash, entertainment portals, and some of the aspects of a personalized, sponsored browser that assists us to the extent that many consider it helpful. Those people don't use the Internet the way the masses do – to watch Netflix, to learn, and yes, most obviously to consume.

We aren't buying, we are being sold. Advertisers prey on this escalating conflation of convenience and benefit. Perhaps this is pessimistic, but even with individual activism, knowledge, awareness, etc. the system will dominate the individual. It shouldn't be about learning to subvert the system. The system will always win. It should rather be about changing the system. That can only come from the top down. The FTC prides itself in protecting the rights of the consumers. Yet its legislation is written to benefit companies. It speaks in terms of what companies can't do. Lines they can't cross. Legislation outlines vague ideas of what is immoral. It protects the companies' interests rather than the peoples'; putting the onus on individuals to regulate themselves, rather than the FTC regulate the corporations.

The government's intrinsic ties to the corporate world are obvious. This change that I hope for is obviously unlikely to happen without some sweeping governmental change and muckraking. It is not how America is set up and run. Still, change needs to come from the FTC, from legislators who listen to their people, from activist groups and the common people.

While McChesney and others advocate for media literacy education in schools, an admirable and essential practice, the reality is that the problems of digital advertising and Internet privacy can only be solved in the context of a larger political revolution. This issue is a symptom of a larger political problem in modern Western society." Regulation must come from the top down, yet the question always remains: How can we make this possible? We know the corporatized Internet is not a progressive force. Companies work for maximized profits and monopolistic benefits. The Internet is growing, but in the wrong ways.

I must acknowledge that advertising needs to exist in order for the Internet to run the way it does. Having people pay to access content just isn't realistic. We live in a capitalistic society that is accelerating. We must understand this, yet realize how to go about things differently. The idealist in me suggests that raising awareness is never a bad thing. IT could inspire a next generation to improve on these rights and regulations. Still, this is not enough. Ultimately, I see what is wrong. The majority of us do. I can propose a solution, but I alone cannot do anything to affect change. Perhaps it is already too late.

I do not take action. I am a hypocrite. I use Google Chrome. I enjoy when my search results come up first. It is convenience. Acknowledgement is useless. Ironically, Europe could be the key to better privacy laws. U.S. companies are so tied to revenue from Europe, that it is possible that when the rejection of the Safe Harbors Agreement threatened their money and power, they began to rethink things. The U.S. government and tech and advertising industries are so tied to one another, that this regulation could not realistically change. Hopefully the EU will continue to develop in the frame of a user-centric, privacy advocating body. Hopefully, the U.S. will be forced to change its privacy laws to reflect Europe's, betting our people's rights on monetary gains.

Pew shows that the common people have given up and given in. Perhaps it is too late. Will something big have to happen to change opinions, or is the convenience factor, the gentle, aesthetically pleasing lull that advertisers have created for users – like a warm blanket with convenient knobs to fill everyone's increasingly immediate and urgent visceral needs – too much to overcome? It seems as if the latter is true. Surely this acknowledgement is extremely pessimistic, but it also feels inevitable. To call for urgency in an age where the majority of users are happy and hypnotized, and one where even those who understand and acknowledge what is happening seem to have become complacent with what exists, simply because it isn't directly harmful and makes us feel good, looks to be pointless.

The regulators need to suck it up. Plenty of people in the FTC believe in what they do. They look to protect the people, the consumers. Yet their definition of protection is flawed when it comes to the capitalistic system the Internet is propagating. As companies more seamlessly integrate their advertisements with entertainment – and it's not just the

Internet, this is our entire world and culture – the last gaps between anonymity, freedom and corporate consumerism will have been filled. It's not just about who's identity is stolen, who's information is revealed to the world to be exploited, who's life and privacy are violated (and that is a huge part of it), it's about the evolution of capitalism into it's final form, one that will change the fabric of how and why we live, how we exercise our right to explore and learn outside of the influence of corporations and brands that control what we purchase and how we think and feel. We are not intrinsically tied to money, but at this rate, we risk exclusively becoming pawns in a system that uses us for nothing more than our dollars.

Yes, we are products right now, but with this continuous infusion, that may be all we amount to and all we think is possible. We won't have choice outside of which brand is best. We won't be able to navigate, learn and explore without our decisions reduced to which company wins us over, which choice we think we want to make. The capacity to think in these ways will slowly fade away. It's about who we become as a people. The government has to recognize this. They have to see us as people, not just consumers who can be reduced to data. The idea that not just our profile, but our predicted and digitally calculated essence can not only be representative of who we are, but also sold as if we are a piece of paper, is threatening to the psyche of the American people. We risk replacing choice with the illusion of choice, freedom with comfort, and curiosity with convenience.

Bibliography

“AdChoices.” *Wikipedia.* Wikimedia Foundation. n.d. Web. 22 Apr. 2016.

“Advertising and Marketing on the Internet: Rules of the Road.” *Federal Trade Commission,* Federal Trade Commission, Dec. 2000. Web. 22 Apr. 2016.

“AdWords.” *Google AdWords.* Google. n.d. Web. 20 Nov. 2016.

“Bloomberg Game Changers.” *Bloomberg.* Bloomberg L.L.P., 2014. Web. Nov. 2015. Video.

Bourne, James. “Online Advertising: A History from 1993 to the Present Day [Infographic].” *Marketing Tech News.* Marketing Tech News, 11 Sept. 2013. Web. Nov. 2015.

Children's Online Privacy Protection Act." Wikipedia. Accessed November 23, 2015. https://en.wikipedia.org/wiki/Children's_Online_Privacy_Protection_Act.

“Digital Advertising Regulation 101.” *IAB Empowering the Marketing and Media Industries to Thrive in the Digital Economy.* Interactive Advertising Beureau, 03 Feb. 2014. Web. 22 Apr. 2016.

Finkelstein, Seth. “Google, Links, and Popularity versus Authority.” *The Hyperlinked Society: Questioning Connections in the Digital Age.* By Joseph Turow and Lokman Tsui. Ann Arbor: U of Michigan, 2008. 104-124. Print.

Krantz, Michael, “The Medium Is the Measure,” *Adweek,* September 25, 1995.

McChesney, Robert Waterman. *Digital Disconnect: How Capitalism Is Turning the Internet Against Democracy.* The New Press. New York, 2013. Print.

Mossberger, Karen, Caroline J. Tolbert, and Ramona S. McNeal. *Digital Citizenship: The Internet, Society, and Participation.* Cambridge, MA: MIT, 2008. Print.

Palrey, John G. and Urs Gasser. *Born Digital: Understanding the First Generation of Digital Natives.* New York: Basic, 2008. Print.

Pariser, Eli. *The Filter Bubble: What the Internet Is Hiding from You.* New York: Penguin, 2011. Print.

Powers, Shawn M., and Michael Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom*. Chicago: U of Illinois, 2015. Print.

Rainie, Lee. “The State of Privacy in America: What We Learned.” *Pew Research Center RSS.* Pew Research Center, 20 Jan. 2016. Web. Feb. 2016.

"Retrospective Review of FTC Rules and Guides." *Federal Trade Commission.* N.p. n.d. Web. 22 Apr. 2016

Schulman, Stacey Lynn. "Hyperlinks and Marketing Insight." *The Hyperlinked Society: Questioning Connections in the Digital Age.* By Joseph Turow and Lokman Tsui. Ann Arbor: U of Michigan, 2008. 145-158. Print.

Schwartz, John. "Giving the Web a Memory Costs Its Users Privacy." The New York Times. September 4, 2001. Accessed November 17, 2015. http://www.nytimes.com/2001/09/04/technology/04COOK.html.

"Skadden Arps. Privacy and Security Update December 2015." *Privacy and Security Update (2015):* 1-8. *Skadden.com.* Skadden Arps. Dec. 2015. Web. Feb. 2016.

"Skadden Arps. Privacy and Security Update October 2015." *Privacy and Security Update Historic New Privacy Shield Agreement Replaces EU US Safe Harbor:* 1-8. *Skadden.com.* Skadden Arps. Jan. 2015. Web. Feb. 2016.

"Skadden Arps. Privacy and Security Update October 2015." *Privacy and Security Update (2015):* 1-8. *Skadden.com.* Skadden Arps. Oct. 2015. Web. Nov. 2015.

Smith, Richard. "The Web Bug FAQ." The Web Bug FAQ. November 11, 1999. Accessed December 1, 2015. https://w2.eff.org/Privacy/Marketing/web_bug.html. - Found via the Electronic Frontier Foundation

"Technological Determinism." *Wikipedia.* Wikipedia, 20 Mar. 2016. Web. 1 Apr. 2016.

"Third-Party Cookies vs First-Party Cookies." Opentracker. Accessed November 27, 2015. http://www.opentracker.net/article/third-party-cookies-vs-first-party-cookies.

Turow, Joseph. *Breaking up America: Advertisers and the New Media World.* Chicago: U of Chicago, 1997. Print.

Turow, Joseph. *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth.* New Haven: Yale UP, 2011. Print.