Online Privacy:

Current Regulatory Approaches, Corporate Responses, and Alternative Proposals

UNIVERSITY OF CALIFORNIA, BERKELEY

LEGAL STUDIES DEPARTMENT

Erica Furer

Honors Thesis

Spring 2012

Professor Chris Jay Hoofnagle

Table of Contents

I. Abstract

Online companies are currently collecting vast amounts of information without the users' knowledge nor their input. Although the collection and dissemmination of this information can lead to a lucrative business, it can also infringe on the users' privacy and give rise to harms such as stalking, cyberbullying, discrimination, and target pricing (Kumari, 2010). To mitigate these harms, it may be best to develop a policy regarding what information the companies can obtain from online users, what methods they can use to receive it, how long they can store it, and what they can do with it. The gateway to understanding and resolving this tension is to investigate how and why companies develop policies relating to users' information. This will be done through the lens of the current proposal by the Department of Commerce, which asks companies to develop voluntary codes of conduct for their actions and policies with respect to user information online.

Through studying organizational behavior of companies and their responses to legislation and previous proposals to change their actions towards consumers and their privacy, this paper offers a critical look at the current proposed solutions and contrast them with an alternative lens – examining the current situation through the viewpoint of antitrust law. This paper examines the premise of whether the unit of currency has now shifted from the physical dollar to information about users, and demonstrates that due to the organizational behavior of companies, coupled with the current industry practices, companies have created a monopolistic market on user data. An alternative policy proposal is then provided to remedy the current situation in which companies are not competing on the unit of commerce, user data. Through scholarly papers, news articles, and transcripts of interviews, this paper examines how corporations shape their policies around privacy and aims to shed light unto the practices for future use in the industry.

II. Introduction

Currently, technology is rapidly changing, corporations are developing new methods to track user data, and the law has not been able to promptly respond and evaluate these new advances at the same speed as they are being developed. Compiling databases of information about users and their tendencies can be very informative and is the primary source of revenue for many businesses in the current digital economy. However, "personal data has come to be a commodity, marketed much as petroleum…" and "each of (the) industries has developed its own system for creation and exchange of personal data" (Rule, 2007). In essence, user data is the vehicle of commerce on the Internet world, but terms of service agreements and privacy policies do not adequately inform consumers how companies are monitoring them and what is happening with the data being collected. Therefore, consumers don't realize that these "free" services, such as Google and Facebook, are not actually free. The commodity that is bought and sold is the personalized user data, which has become valuable in the Internet economy.

Both young and older adults agree that "there should be a law that gives people the right to know everything that a website knows about them" and "that there should be a law that requires websites and advertising companies to delete all stored information about an individual" (Hoofnagle, King and Li, 2010). The current situation is that most Internet users believe that the United States either has or should have protections for them regarding the information that companies obtain from their daily activities on the Internet. On the side of the government, there is currently a proposal by the Obama Administration to have the Department of Commerce "convene the I3S [internet and information innovation sector] and related sectors and industries to facilitate the development of voluntary Codes of Conduct" (The Department of Commerce, Internet Policy Task Force, 2011). In this proposal, the I3S "is comprised of companies, from

small businesses…to large companies that only exist on the Internet" and these Codes of Conduct, are a voluntary reccommendation, not an actual piece of legislation (The Department of Commerce, Internet Policy Task Force, 2011). Although the answer to identify the harm of privacy intrusions has been the crux of many lawsuits in the past decade and has been difficult to pinpoint to enable developing effective legislation, one overarching point is crucial to make about these arguments. Just because consumers aren't acting out, it doesn't mean that they don't care or consent to tracking, but rather it can be attributed to lack of awareness of the tracking. Therefore, transparency and education are a large part of this equation to solve the problem. However, it is also important to remember that education is not the whole picture in the current situation because informing users alone will not change industry practices. Presently, industry practices and perceptions of what is acceptable ultimately determine the level of privacy intrusions.

The disconnect between what the consumers expect and the level of privacy protection that the government is providing is immense. However, because of the speed of innovation, the government does not always have adequate information to be able to affirmatively regulate the technology sector. The most knowledgeable people are those in the industry - the corporations, because they control the physical information and are the ones determining how to implement the new technologies. Therefore, studying their policies, practices, and responses to new technologies and regulations are the methods to understanding and resolving the dilemma between the users, corporations, and the government.

Many of the corporations see privacy protections (or lack thereof) as being a direct outcome of market forces. Paul Misener, the Vice President on Global Public Policy for Amazon.com, testified that the reason for their privacy policy is solely because "privacy is

important to our customers, and thus it is important to Amazon.com. We simply are responding to market forces" (Misener, 2001). He also stated that if Amazon.com failed to "provide the privacy protections [consumers] demand," then they would shop at "established brick and mortar retailers," Amazon.com's "biggest competition" (Misener, 2001). However, Amazon's rationale that their only reason for having a privacy policy is to be able to compete with offline competitors cannot explain for companies such as Google, who do not have offline rivals but still found the need to have a privacy policy. One explanation is that these companies view privacy as a legitimate concern and an intrinsic value in our society as Warren and Brandeis did in 1890, and therefore they want to protect their consumers from having their privacy violated because it's the right thing to do (Brandeis and Warren, 1890). However, constructing databases of information about consumers, which help companies develop their marketing platforms, has turned into a lucrative business worth billions of dollars. Therefore, this altruistic theory can't explain why most companies, who are inherently profit maximizing, would adopt a privacy policy which restricts their ability to profit off of information.

This paradox is what brings me to my research. First, I will examine some background on the industry's viewpoint and what the dilemma is consistently being framed as – protecting user privacy versus the ability for the advertisement agency to be efficient and maximize profits. Next, I will examine some theories regarding organizational behavior to aid in evaluating contrasting proposals. This paper will then provide some critical analysis at the current stage of the Department of Commerce's proposals and suggest an alternative to remedy the potential flaws. The aim is to evaluate what the most effective means of organizational response to protect consumers is in the growing digital age and to ensure that companies don't subvert the policies.

III. The Industry's Perspective

Online companies and advertisers have the rationale that obtaining information from consumers by way of tracking their behavior enables marketers to more efficiently convey information to consumers who are more likely to buy their products. Consumers are then directly targeted with ads pertaining to products that they are actually likely to buy. Furthermore, in a discussion forum regarding the Do Not Track proposal, Mike Zaneis, Senior Vice President and General Counsel for the Interactive Advertising Bureau, developed the argument that "publishers and content owners have every right, in fact have fundamental rights, to offer their goods and services as they see fit" (Zaneis, 2011). The line of logic is that in Article I, Section 8, Clause 8 of the United States Constitution, Congress is charged with promoting "the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." Known as the Copyright clause, this passage has been interpreted to mean that authors have the right of exclusivity of their copyrighted material, and as per Mark Zaneis, that authors have "the right to …offer access to your work under your own terms, including charging a fee for requiring viewers to allow advertising" (Zaneis, 2011). This "fundamental right" of copyright, along with the ability of a service provider to determine the Terms of Service agreement, are the pretexts for why some companies disallow consumers from entering their websites if the consumer uses ad blocking technologies. From the industry's perspective, companies have the right to refuse service because these ad-blocking technologies "fundamentally impair their ability to monetize their content" (Zaneis, 2011). This phenomenon will be revisited near the end of this paper.

Another practice occurring in the discussion surrounding online privacy is that companies are trying to differentiate themselves as being more privacy friendly than others.

Social media companies such as Facebook assert that they do not collect any information from consumers secretively because all the information Facebook collects is from what the users post about themselves and their friends to others. In a recent interview with Charlie Rose, Mark Zuckerberg, founder and CEO of Facebook, said that companies like "Google…have search engines and ad networks … also have a huge amount of information on you, it's just that they are collecting that about you behind your back…you're going around the web and they have cookies and are collecting a huge amount of information about who you are but you never know that… it's less transparent than what's happening on Facebook. [On Facebook, people choose who to advertise to based upon the user defined preferences] … On the other services, those companies collect the information and choose for the advertisers who they will show the advertisements to – they have no control over the information that the company has about you" (Zuckerberg and Sandberg, 2011).

In their description of Facebook as not tracking users "behind their backs," Facebook left out a crucial element of their own product – the Like button. Facebook gives other websites the opportunity to place a Like button on their website, which allows Facebook users to click the button and the link is subsequently placed on their Facebook page. This functions as a great marketing tool for businesses because it serves as a personal referral for a product to potential customers coming from their own friends. However, researchers discovered that the "Like button is also used to send cookies and to track and trace web users, regardless of whether they actually use the button. The browsing behavior of individuals can be connected to their Facebook account. If a user has no Facebook account, a separate set of data concerning individual browsing behavior can be created. When a user creates an account later on, the data can be connected to the newly established profile page" (Roosendaal, 2012).

Therefore, even the rhetoric of the companies is not accurate when making statements for the public to truly understand their product and its level of privacy intrusion. Even companies that contend that they do not use your information without your knowledge have practices that violate their own statements. The industry argues that if the consumer doesn't care about being tracked, and their information gives them more relevant advertisements and coupons, then why prevent this from happening. On the contrary, as per the industry, methods of tracking should not be regulated because it would impede innovation of new and more efficient methods of advertisement and more convenient products for the consumer. However, companies are continuously attempting to paint themselves as concerned about user privacy, and therefore there must be a reason why the privacy issue keeps surfacing. A further exploration of the industry practices will shed light unto why the practice of companies tracking users to identify them is contentious.

IV. Current Industry Practices

Proposals have been brought forth throughout the marketing industry that companies should treat customers differently depending on how much they spend (Selden and Colvin). The intent behind these proposals is that if the company can market more to more loyal customers who tend to spend more, then they will make much more profit because those consumers are more likely to spend more. Joseph Turow describes the ways that firms obtain the information on consumers from multiple data sets, anonymize them, and then sell them to companies for effective marketing (Turow, 2011). Companies such as Next Jump, Rapleaf, and The Daily Me provide predictions on the reliability of individuals based off of data they compile from social networks, information from the human relations departments of corporate employees' companies, and credit companies (Turow, 2011). This compilation of data is then sent to companies with the intent to be able to offer consumers different ads, offers and prices, so that companies can "learn how to find and keep the most valuable customers by surrounding them with the most persuasive media materials" (Turow, 2011). Turow argues that this "strategy of social discrimination will increasingly define how we as individuals relate to society – not only how much we pay but what we see and when and how we see it" (Turow, 2011).

Another way of obtaining information about consumers that relies solely on consumer activity online is behavioral targeting. This typically works by way of advertisers creating "behavioral segments to describe users' online activities, and then, when the user visits other sites, the advertisers place ads for products that relate to the behavioral segment with which the user is identified" (Gross, 2010). Each user is then tracked according to the websites they visit and their keyword searches in order for the advertisers to be able to show consumers ads based on their past online history for more efficient marketing (Gross, 2010). Behaviorally targeted ads

have significantly higher prices than standard advertising because they is a much more directed and efficient way of marketing to the consumer and are "more likely to tell them about a product they want to buy" (Beales, 2010). According to a study of twelve large advertising companies, behavioral targeting accounts for approximately 40 percent of the average ad network's revenue, and is a very commonly used practice in the industry (Beales, 2010).

However, this behavioral advertising relies on identifying the user and tracking them over the span of their actions online, not just their activity on one particular website. This exemplifies how online advertising is different from traditional offline marketing. Yes, the marketing serves the same purpose of informing consumers of products, and offline channels attempt to optimize their advertisements by picking certain times of day or channels on television, or appeal to a certain market by choosing the newspaper or magazine to advertise in, but online marketing is distinct from offline in the way of being able to create a profile of information about users based off of their aggregate behavior. Brick-and-mortar stores can catalogue their buyers' previous purchases in their stores and attempt to tailor advertisements on this basis, but online advertisers can market to consumers based off of their actions and purchases on almost all the websites they go to. This fundamental difference makes the advertising so much more efficient, but studies have shown that online, it is "easy to link tracked information with an individual's personally identifying information" and therefore users' information from one website is available to advertisers and services even when they did not intend to share that information with anyone else (Backes, Kate and Maffei, 2012). The harm to the consumer that could arise from this would be "a less favorable offer, denial of a benefit, or termination of employment" (Mayer and Mitchell, 2012).

Other privacy advocates have also identified other harms of tracking users, but the crux

has been to find actionable grounds on which to bring a lawsuit against companies for privacy intrusions. Lawrence Lessig argues, "private data flows too easily… it too easily falls out of the control of the individual" (Lessig, 2002). He points out that in the case of copyright, it's a felony to publish more than a certain amount of work without permission because it's seen as property (Lessig, 2002). Therefore, Lessig believes that personal information should be viewed as property and therefore it would not have the problems that are persistent today. (Lessig, 2002). A 2012 survey by Pew Internet reported that 68% of respondents were "not okay with targeted advertising because [they] don't like having [their] online behavior tracked and analyzed" (Purcell, Brenner and Ranie, 2012). Therefore, the problems are persistent because of the ease that data can be transferred, but consumers themselves do not want this targeting that they consider to be invasive.

Gary Locke, the secretary of the Department of Commerce, stated, "Web users need to be confident their personal data is secure and not being misused. … Self regulation without stronger enforcement is not enough, consumers must trust the Internet in order for businesses to succeed online" (Gross, 2010). Therefore, it is necessary to see how companies react to regulations to see what the best enforcement mechanism would be for securing the privacy of consumers online, which can be done through the study of organizational behavior.

V. Corporate Responses to Regulations

A. Law as a Standard

The interaction between companies and regulations is a large part of the study of organizational behavior. The theory of neo-institutionalism suggests that organizations adopt regulations and standards and "obtain legitimacy by conforming to institutional and market pressures within their business environment" (Appari, Johnson and Anthony, 2009). Lauren Edelman describes how organizations themselves create standards, which she calls "managerialized law," that "reenter legal fields and affect the thinking of judges and the rulings of the courts" (Edelman, 2007). She states that law is "endogenous, constructed in and through the organizational fields that it seeks to regulate" (Edelman, 2007). In the current case of corporation's policies reacting to new technological developments, the scenario that has developed is that absent a law, organizations have created their own practices. However, these practices have influenced the law by preventing it from being developed, as evidenced through the absence of a comprehensive Federal privacy law. Corporations such as Amazon.com and the Digital Advertising Alliance have pushed for regulations to not be enacted and have stated that they regulate themselves, which is where the problem lies currently. An example of this circumstance is the discussions on the Do Not Track proposal.

Do Not Track is an opt-out proposal, which means that all users' online activities will be "tracked" unless they specifically designate otherwise by clicking the "Do Not Track" button placed on the website. Different proposals by browsers exist for implementation. Domain blocking is one proposal, in which the user enters domains and instructs the browser to never contact them (Bilenko, Richardson and Tsai, 2011). The other two proposals are opt-out cookies and HTTP headers, in which the "browser contacts the target domain but informs it that the user

wishes not to be tracked" (Bilenko, Richardson and Tsai, 2011). The policy portion of this proposal "defines what websites must do when they receive a Do Not Track header" (Mayer and Mitchell, 2012). The proposal outlines that all of the browser controls would be clearly explained for the users to make an informed decision. However, critics of the proposal argue that users will not be completely informed by the practices and could be confused because Do Not Track is focused on behavioral tracking, and not necessarily other forms of tracking. For example, contextual advertising, when the advertiser scans the content of the website the user is viewing and places the ads from this information, would not be prevented by Do Not Track. Also, the proposal "neglects tracking performed for non-advertising purposed (e.g., data collected could be used for differential pricing on retail websites)" (Bilenko, Richardson and Tsai, 2011). These arguments are a few of the many concerns of the Do Not Track proposal, but what is of note is the organizational development and response to the proposal from key industry players.

"The White House recognized that user privacy protections are nearly useless without a method of enforcement, so it has reaffirmed that companies that commit to respecting Do Not Track will be subject to Federal Trade Commission (FTC) enforcement" (Reitman, 2012). However, the Digital Advertising Alliance "added another exception into their promise to respect Do Not Track: they won't respect the setting unless a user affirmatively chooses Do Not Track and won't respect it if 'any entity or software or technology provider other than the user exercises such a choice'" (Reitman, 2012). Therefore, the default must be opt-out for this Do Not Track provision because otherwise the Advertisement industry would not accept it. This effectively shows that no matter what kind of self-regulatory code is implemented, when all the industry stakeholders are being pleased, the consumer's privacy is not held paramount. The organizations prevent the law from being developed because they control what occurs in the

industry. Because Edelman's theory comments on how organizations internalize the law and how it is developed, and this has not occurred yet, it is necessary to take a step back and examine what explains for the occurrence of the standard in the industry today.

B. Emergence of a Standard Without Law

Institutional Isomorphism is the theory that "once a field becomes well established … there is an inexorable push towards homogenization" (DiMaggio and Powell, 1983). In the context of online privacy, this implies that once one company adopted a standard (or taking an example, developed a privacy policy), the rest followed suit not because they did the research and it was best for them to do so, but rather because they just adopted the policy of the competitors to be able to compete in the marketplace. Amazon's case can also be explained with the theory of institutional isomorphism if the other brick and mortar companies originally provided services with a guarantee of privacy, so Amazon followed suit to also ensure privacy and to be able to compete with them. They had to develop something to stay in the market as a trusted source, so this is the reason why Amazon.com developed a privacy policy.

However, it is unclear as to who was the first company online to have a privacy policy and therefore it is difficult to know if Amazon just followed the other companies or developed the privacy policy to compete with the brick and mortar stores. Taking the first explanation, there are three scenarios within DiMaggio and Powell's accounts of institutional isomorphism, which explain for how the homogenization of an industry can occur and why. The first is coercive isomorphism, which arises from "political influence and the problem of legitimacy" (DiMaggio and Powell, 1983). This occurs when organizations are influenced by conformity to wider institutions such as the state or federal laws. Their third scenario is normative isomorphism, in which "government recognition of key firms or organizations may give them legitimacy and

visibility and lead competing firms to copy aspects of their structure or operating procedures in hope of obtaining similar rewards" (DiMaggio and Powell, 1983). Both the first and the third scenario account for the homogenization of an industry when there are external factors relating to governmental regulation or intervention, and the development of the industry regarding consumer online privacy has largely not been an influence of direct governmental regulation.

Instead, the second scenario of mimetic isomorphism is "when key technologies are poorly understood, or goals are ambiguous…[and therefore] organizations may model themselves on other organizations" (DiMaggio and Powell, 1983). The original corporation may be "unaware of the modeling" or may have "no desire to be copied; it merely serves as a convenient source of practices" that other corporations use (DiMaggio and Powell, 1983).

This theory would apply to the case of online corporations if the problem that arose were a lack of privacy legislation, which made the firms in the industry uncertain as to which course to take next. The question that follows is that in absence of regulation, what spurred all these companies to make privacy policies. One explanation is that of institutional isomorphism – that once one company did it, the others just followed suit. However, in this model, there is a first – the original company that adopted a privacy policy and was allegedly "driven by a desire to improve performance" or had some sort of impetus that drove them to adopt this policy (DiMaggio and Powell, 1983). In this theory, the following companies did not reassess how to meet their needs efficiently and just basically took the privacy policy from the first company. This becomes dangerous when, as described earlier, there is no motivation from an industry to change its policies when the practices change. James Rule addresses precisely this problem when he states "privacy codes rarely challenge basic premises of institutional surveillance. They

implicitly accept the legitimacy of institutional collection and use of personal data, in response to what are often vaguely bracketed as organizational “needs” for such information” (Rule, 2011).

VI. Potential Harms

If one company would change their privacy policy when their technology changed on their own virtue, as per the theory of institutional isomorphism, the other companies would change their policies too and the industry would self-regulate. However, if there were no incentive for the first organization to change or create a new privacy policy in light of their changing methods of gathering information from users, then other corporations would not follow suit. This is where the statement by Amazon to the FTC that "the market forces are working and … there is no need for legislation" becomes harmful to society (Misener, 2001).

However, "if people do not notice an attribute [or it is not disclosed to them in an obvious manner], it cannot have an impact on the decision process" (Nehf, 2007). When there is such a power differential that consumers are not even aware of the possibilities of use and abuse by corporations of their information, then the consumers will not have a stimulus to send the market signal to the companies to change their privacy policies (by not purchasing from them). This information asymmetry leads to companies not changing their privacy policies or practices on collecting personal information or self-regulating, which is where the harm lies.

Furthermore, even if the consumer proactively sought out to fully try to understand what information companies collect and what it is used for, "web site users lack the information necessary to evaluate the risks of information sharing" (Nehf, 2007). Education and awareness of the ways information is used and the implications of disclosing information is crucial to remedy this issue because currently, there is not enough information being placed on the websites for the average user to be able to make an informed and rational decision. Consumers with more education and technical knowledge are more likely to be more privacy conscious and

refuse to share information online, but even then, "most privacy policies are obtuse and noncommiting, but even a straightforward policy can be deceiving" (Nehf, 2007).

For example, Ben Edelman has examined how companies have violated their own privacy policies, even with all their ambiguity, in a multitude of studies. One of his more recent ones was examining the Google Toolbar, where he found that it still tracks people's browsing, even after the users disabled the feature (B. Edelman, 2010). The response to this study was that Google simply changed the coding for this one specific problem – there was no further investigation or inquiry on its other practices.

A. Circumvention of User Choice

Another example of companies subverting industry practices was uncovered by researchers from UC Berkeley in 2009. Industry advertisers found that users were automatically deleting their HTTP cookies once a month, which would disable them from being tracked. Therefore, advertisers reacted by developing another form of tracking the user – Flash cookies. These Flash cookies were favored by the industry because they would persist for longer amounts of time by not being deleted by default, and because users weren't aware that Flash cookies existed, they had no impetus to delete them by themselves. In their study, the researchers found "that the top 100 websites are using Flash cookies to…recreate deleted HTTP cookies" which meant that even users who were conscious about their privacy and attempted to prevent any tracking could not do so, and did not even have the knowledge that it was occurring (Soltani, Canty and Mayo). Privacy policies did not disclose any presence of Flash cookies and therefore even if a consumer had attempted to clear all cookies and took actions to prevent any tracking, the websites were still tracking them. "Advertisers were deliberately subverting the clearly stated preferences of consumers" (Temple, 2011).

What occurred after this report was released followed the same trend as the response after Ben Edelman's unearthing of the Google privacy violations. After the exposure of the practice, Flash cookie use declined, but shortly after, "marketers (were found to be) using new tools for essentially the same purpose" (Temple, 2011). The industry reacted to the proposal by eliminating just the one particular method of tracking (Flash cookies), but still perpetuated the practice of tracking users, which is precisely what researchers did not want to happen. Marketers would develop strategies to track users because there was (and still is) no prohibition against tracking, and once the strategy was caught, they would just move on to the next strategy.

This cycle is apparent in examples throughout the industry. The Wall Street Journal's *Did You Know* series describes many of the privacy intrusions that companies are engaging in; such as iPhones storing location information even when the services were affirmatively turned off and "supercookie" tracking that is almost impossible for users to detect occurring on popular websites such as MSN.com and Hulu.com. Google was investigated for" bypassing the privacy settings by million of users of Apple Inc.'s Safari Web browser…[but] Google stopped the practice last month after being contacted by The Wall Street Journal" (Angwin, 2012). These are just a few of the numerous examples that display this pattern of circumvention of user choice until caught. This phenomenon demonstrates that companies circumvent both user choice and industry practices to ensure the maintenance of the ability to collect user data without many restrictions, and that this is the default.

B. Denial of Harms of Tracking

In her testimony, the Chief Privacy Officer of IBM stated that the Federal Trade Commission should not enact legislation based off a "vague notion that data collection itself is

harmful" (Pearson, 2001). This statement shows the asymmetry of information that the courts, citizens, and regulatory agencies have as compared to these corporations. There is no way to assess how the data collection can be harmful without looking at the processes of the collection themselves and what the data is used for and who it is disseminated to. However, since the privacy policies are not even required to disclose all of this information and have been shown to not always reflect the current practices, then it becomes very difficult for consumers and regulators to have anything but a "vague notion" that the collection of data is harmful.

It's not necessarily the act of collecting data that is the problem, because it can help efficiency of an industry as many advocates have stated. However, circumvention of user choice is the problem, and because of the organizational behavior that once one company creates a way to bypass user choice and profit off the data, all the other companies are compelled to do the same because they cannot be left behind. Because there is a lack of regulation of the industry, this practice is commonplace. Therefore, institutional isomorphism may be able to account for how the present situation of most online companies having a privacy policy has developed, but this paints a very grim future of symbolic compliance if these practices are not examined deeper. What the Department of Commerce is attempting to do with the Codes of Conduct is precisely to ensure that there is some self-regulation in the industry that has to abide by certain policies. However, if what is and will be occuring is simply mimetic organization, it seems as though there needs to be some sort of proactive way to prevent companies from circumventing user choice such as regulatory body present to investigate the current practices of companies to ensure that they have not developed new tools of tracking and surveillance. The following proposals are attempts to remedy this issue. The first alternative is for the Department of Commerce to help

develop the overarching codes of conduct, and the second is to attempt to bring the users in as the regulators and apply an antitrust view to online privacy.

VII. Department of Commerce Codes of Conduct

The Department of Commerce released a Green Paper in December of 2010, which outlined a process in which multiple stakeholders would engage in creating a completely voluntary "code of conduct" to help secure consumers on the Internet (The Department of Commerce Internet Policy Task Force, 2010). This proposal also recommended the development of a Privacy Policy Office within the Department of Commerce to oversee these developments. Since this report, the Federal Trade Commission has brought enforcement action against online companies that failed to honor opt outs because "the orders in these cases are designed to ensure that when consumers chose to opt out of tracking by advertisers, their choice is effective" (Federal Trade Comission, 2012). This seems to remedy the circumvention of user choice issues that the previous researchers had pointed out. The FTC also stated that it continued educational efforts and that many Internet browsers developed ways for consumers to send requests to websites for them to not track their activities. The Department of Commerce has not described their codes as regulations "in order to make the process attractve to business groups…but consumers should know that the rules will be enforceable" (Gross, Commerce Department Will Push Privacy Codes of Conduct).

A. Potential Flaws in the Codes of Conduct

The main criticism of the Department of Commerce's proposal of Codes of Conduct is that "the report offers a "vague multistakeholder process" to develop codes of conduct instead of real laws to protect consumers," said Jeffrey Chester, executive director of the Center for Digital Democracy. … The report should have also "rejected outright any role for self-regulation, given its failures in the online data collection marketplace." (Gross, 2010). As was discussed earlier, companies develop new technologies, and only once researchers discover the practice occurring,

then the company reactively changes their policy. Therefore, because the industry has demonstrated it's mimetic isomorphism tendencies, another criticism of the proposal is that simply educating users and making people aware of industry practices does not solve the problem. Having any sort of reactive action by a regulatory body that does not proactively bar tracking from occurring will not be effective.

B. Do Not Track

As was mentioned previously, Do Not Track is a large tenant of the privacy conversation that the Department of Commerce is constructing, and is "dependent on companies agreeing to play by those rules – it is a voluntary system" (Bradley, 2012). Furthermore, the whole premise of opt-out provisions such as this one are subject to much scrutiny. "There is still something inherently wrong with a system that automatically assumes you want to be spied on until or unless you figure out where the Do Not Track button is for your browser and make the effort to enable it," wrote Tony Bradley in an article in PC World, and much of the debate around opt-in versus opt-out provisions have centered around this issue (Bradley, 2012). Currently, the standard is that companies assume that if there is nothing specifically prohibiting them from collecting information, then they may go to any extent to obtain information and assume that the users agree with it.

However, the President and CEO of the Interactive Advertising Bureau, Randall Rothenberg, "attacked the W3C process and the Do Not Track flag, warning member companies it could "kill" their businesses" (Reitman, 2012). Jonathan Mayer, a researcher at Stanford University, tested this hypothesis and explored the impact that Do Not Track would have on the advertising industry. Because Do Not Track would only account for third-party tracking, he discovered that the proposal would only account for 4% of US online advertising expenditures

and would only affect the people who choose to opt-out (Mayer, 2011). The fear by the advertising industry that Do Not Track will cripple their profits is still the impediment to form legislation due to the explanations by the organizational behavior theory, even though it has evidence that would suggest that implementing the proposal would not have a detrimental impact on the industry.

"You should just assume that if you post it, share it, access it, or store it online that it's probably going to be seen by some unauthorized party at some point" (Bradley, 2012). In the current situation, this is the reality because the industry sees it as this, and so the only solution right now is to "simply choose not to do business with sites or services that violate your trust and breach your privacy," as per Tony Bradley (Bradley, 2012). However, as was discussed previously, the only real way that consumers can find out that about privacy intrusions is from an external source – either academics or regulators have to discover the breach and then disseminate the information to consumers. Due to the cycle of companies fixing the problems only once they are pointed out, if a privacy intrusion is discovered, then the company ceases to use that particular technical mechanism and when the consumer is made aware that it was occurring before, the problem is fixed, which gives them the illusion that their privacy is held paramount by the company. Therefore, these privacy breaches occur and the consumer has almost no way of discovering the privacy breach on their own, and if they are made aware of the intrusion post facto, the problem would most likely be already solved and therefore not trigger a loss of "trust" in the company.

Furthermore, in the current state of development, at least of the United States, consumers do not have the choice to "Exit" markets that they are not comfortable with. When the standard is to collect as much information as possible, all the companies need to do so to remain

competitive, and therefore if a consumer would like to not patronize those particular companies, then they are left with almost no sites that they can visit. Therefore, the consumer needs to be made aware of the extent that they are being tracked, and there need to be alternatives for them to be able to exercise choice of what they would like to use according to how much privacy they need to give up for it. Herein lies the set-up for the alternative to the Department of Commerce's self-regulatory proposal. The real research question has now developed to be: what is the most effective means of organizational response to protect consumers in the growing digital age and to ensure that companies don't subvert the policies?

VIII. User Data as the Governing Commodity

Because of organizational behavior and lack of any proactive legislation, companies' mentality is that the most information they can acquire from the end user is best, and therefore there is no ideological limit to how much information they will collect, or the methods that they will use to obtain it. However, an alternative view of the transformation of business online lends itself to a solution for the online privacy problem. "Content owners already charge users for access to some content and services" because if a user has blocked ads on their browser, then the service needs to acquire money somehow (Fisher, 2010). Therefore, these content owners already acknowledge that the way they earn money is through advertisements, and the more direct and tailored an advertisement can be, the more that marketers will pay for that spot. Therefore, the user's information is really the commodity being bought and sold in the new online market.

A. How Much is User Data Worth?

According to Experian, in March 2012, not including mobile traffic, "Facebook had more than 7 billion total visitors; Twitter had 182 million; and Pinterest had 104 million total visits from people in the United States" (Sutter, 2012). The major way that these companies generate revenue is through advertising, and Facebook stated in their IPO documents that in 2011, "they made $3.15 billion of $3.71 billion solely from advertising" (Jaycox, 2012).

However, the current valuation of user data for buyers is extremely low. "User profiles -- slices of our digital selves -- are sold in large chunks, i.e. at least 10,000 in a batch. … They go for $0.005 per profile, according to advertising-industry sources" (Madrigal, 2012). There are two models for marketers to pay for accessing the consumers. One is pay-per-click (CPC) where the advertiser sets the maximum amount that they are willing to pay for each user click, and

therefore only pays when this occurs. The other model is pay-per-1,000 impressions (CPM), so the advertiser pays a standard fee for every 1,000 times their ad is displayed on the website, regardless of the number of clicks. LinkedIn's minimum CPC bid is $2.00 per click and the minimum CPM bid of $2.00 per thousand impressions, with a minimum daily budget of $10 (LinkedIn, 2012).

Therefore, just being given the opportunity to reach consumers can be extremely costly because these websites such as, "Facebook and Google make roughly $5 and $20 per user, respectively. Without your data in one form or another, their advertising would be mostly worthless, so perhaps your data is worth something in that range. But let's not forget the rest of the Internet advertising ecosystem either; which the Internet Advertising Bureau says supported $300 billion in economic activity last year. That's more than $1,200 per Internet user and much of the online advertising industry's success is predicated on the use of this kind of targeting data" (Madrigal, 2012). This analysis shows the inconsistency between the amount of data that is being collected, the vast profit companies are making on the use of the data, and the amount that is being charged for it. If users were to be able to control that, then this could increase the value of the receiving of the information, making it sell for more, and putting the power into the consumer's hands.

The results of a conducted study demonstrated that, "people who think they have already lost the ability to control private information ... may value privacy less" (Madrigal, 2012). In this study, users responded that they would not pay money to stop companies from using their information, but would also not accept money to allow companies to start collecting information about them. Therefore, if users are asked before their privacy is infringed upon, they may value privacy more than those who feel that the privacy has already been eroded. Therefore, "the

companies making the data-tracking tools have serious incentive to erode the idea of privacy not just because they can make (more) money, but because privacy erosion leads to more privacy erosion. The system is self-reinforcing. This is a problem" (Madrigal, 2012).

The key to ensuring privacy protection for consumers is then to ensure that users have the choice of deciding the use of their information before they use the website or service. An opt-in strategy would achieve this goal – to have users only be tracked if they affirmatively choose that option. However, the online advertising industry, as demonstrated, thrives on being able to target consumers in multiple ways, and therefore would be extremely unlikely to consent to an opt-in method. Therefore, there needs to be a solution that ensures that users can set their preferences very explicitly prior to the website engaging in any sort of tracking or targeting, that companies do not circumvent user preferences, and that companies keep users aware of the practices and require consent for new methods before being implemented. Up until this point, the cycle has been to track users until a regulator discovers the tracking. This is where the harm lies – with the voluntary proposals by the Department of Commerce, new technologies and methods of tracking which the consumer is not aware of would not be prevented but rather would only be stopped once discovered. This places an immense burden on the regulators and academics to engage in a policing activity of the industry.

However, examining this problem through the lens of antitrust could mitigate many of these issues by making the consumers the regulators and ensuring that companies compete on privacy, which would in effect restore the buying power to the consumer and allow them to capture the value that is in their data.

IX. Antitrust Lens as the Solution

The aim in this section is not to establish a cause of action for an antitrust lawsuit against all the websites in the industry for monopolizing user data, although this is in effect occurring. User data is the vehicle of commerce on the Internet world. However, consumers don't realize that these "Free" services, such as Google and Facebook are not actually free. The commodity that is bought and sold is the personalized user data, which becomes valuable in the Internet economy. "The FTC wields significant soft power that complements its enforcement activity…and can threaten enforcement … or publically call on businesses to improve their practices" (Mayer and Mitchell, 2012). What this section proposes is a more theoretical approach by using an antitrust lens for examining this issue of user privacy from the perspective of the monopolization of the current unit of commerce on the Internet.

A. Governing Antitrust Laws

Antitrust law historically began with the Sherman Act of 1890, which "outlaws every contract, combination, or conspiracy in restraint of trade," and any attempt at monopolization (Federal Trade Commission, 2012). There are both civil and criminal penalties for violations of the Sherman Act of up to $100 million and up to 10 years in prison (Federal Trade Comission, 2012). The other governing law for antitrust actions is the Federal Trade Commission Act, which "prevents unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce," and allows the Federal Trade Commission to "prescribe trade regulation rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices" (Federal Trade Comission, 2012). The third governing law of antitrust is the Clayton Act, which specifies rules regarding mergers and acquisitions of companies that may lessen competition. The "rule of reason" balances efficiency

versus the harms of a monopoly and if it can be proven that a company provides a service more efficiently by being a monopoly, this can be a defense to an antitrust charge (Scotchmer, 2011).

B. Antitrust as Applied to the Internet (Google and DoubleClick case)

The most common approach to antitrust law currently is attempting to block companies from merging in fear of monopolistic behavior. The major case regarding antitrust as applied to the internet and taking privacy into account was in the debate on whether Google could acquire DoubleClick, a company which posts advertisements all throughout the internet and therefore collects a vast amount of data from consumers. The privacy advocates, along with even a Commissioner of the Federal Trade Commission, Pamela Jones Harbour, had concerns with this action on the grounds that it would enable Google to have a near monopoly on user data, thereby violating the Clayton Act. However, these critiques did not prevent the acquisition and on March 11, 2008, Google officially acquired DoubleClick (Google, Inc., 2008).

Antitrust law is conventionally seen as the body of law that prevents companies from dominating the market too much, and that has the power to break up these monopolies to introduce competition to the market. This paper does not contest that there are alternatives to every search engine or social media company, and that each of these companies have their own ways of obtaining user data. Therefore, the monopoly is not of information by one company. However, it is necessary to harken back to the other two antitrust laws – the Sherman Act and the FTC Act. As Peter Swire described it, there are two types of market competition – price competition and non-price competition (Swire, 2008). In the online world, companies are not competing off of price in the contentional sense because users are not being charged money in order to access sites such as Facebook and Google. However, users are giving up a commodity in exchange for the service, and that is their personal information (Whittington and Hoofnagle,

2012).

C. Organizational Behavior as Applied to Antitrust Law

If we look at the amount of personal information a company has on its users as the factor determining its value, we can see that currently, companies are not competing based on this elemental unit of commerce. As demonstrated, companies are not competing because there is virtually no restriction as to how much data they can collect from users, and the default is that they can collect as much information as possible. Therefore, companies online will continue to collect an unrestrained amount of data because this is how they monetize their value - through advertisement. Because of the previous investigation into companies' behavior in response to regulation, even if the FTC or the DOC tried to regulate the methods or amount of information collected, it is highly likely that the companies would simply find a different way to collect the information, akin to what happened in the Flash Cookie example. Therefore, what can be observed is a complete lack of competition based off of the unit of commerce, which gives no incentive for companies to restrict their collection of user information. The users therefore effectively have no alternative but to have their information collected by the company and have no voice in the amount of collection or methods, and no way to exit this market absent almost completely shutting off the Internet, which is not a realistic option in this increasingly digital world.

Antitrust law, although typically seen as solely preventing mergers and acquisitions, specifically outlaws every contract, combination, or conspiracy in restraint of trade as per the Sherman Act. Therefore, because the default is to not compete on the unit of trade, the practice of unrestrained collection and use of information without user consent is akin to a conspiracy in restraint of trade and competition. To employ a parallel to the physical world – the current

practice of companies not informing users of the amount of information that they are obtaining from them and what it is used for is akin to all physical companies having access to people's bank accounts, and taking money out of the account without the user's knowledge of how much is being taken out or what it is being used for. The companies would simply say to the consumers, "we need some money to be able to provide you with the goods you want, and we already have devised a way to access your bank accounts," and then without the user allowing access to their account, the company would, by default, withdraw their money. However, it would not just withdraw the amount of money they need to produce the product, but rather would not inform the users of how much they would take. If all companies were engaging in this practice, then there would be no impetus for them to change their actions because they are profiting so immensely off of the fact that there is no competition for price. Unless consumers affirmatively knew about this practice and explicitly told the company to not get money from their account, each company could take an unregulated amount of money from each consumer, so there would be no competition on the price of their products, which would certainly be considered a non-competitive practice.

However, in the physical world, it's easy to know how much money was taken from your account, who took it out, and by what methods. However, in the online world, this is loosely what's happening but with one major exception – users do not have a way of "checking their accounts" or knowing when their information has been taken or by whom. Online companies take an almost unregulated amount of information without the affirmative consent from the user because they have direct access to the user behavior and technical methods of extracting and tracking the data and behavioral patterns. The collection of data is the mechanism that allows companies to collect their revenue, and they are engaging in these almost unrestrained methods

of collection of data which is completely anti-competitive: the default is collecting as much data as possible.

D. Consumers As Regulators

Therefore, the way to solve this antitrust problem is to develop a mechanism in which consumers would be able to affirmatively select what information is given and how, and for the company to adhere to those policies. Through online surveys, laboratory studies, and field studies, Janet Tsai discovered that if "privacy information [is displayed] alongside search results, users will be more likely to visit websites that have high levels of privacy" (Tsai, 2009). Having a high privacy rating significantly raised the amount of users willing to use a site, and sites with privacy indicators attracted many more people than sites without it (Tsai, 2009). Therefore, the conclusion of this study was that "privacy indicators have an impact on which website a user decides to visit" (Tsai, 2009). This experiment ran multiple iterations, each testing the strength of user desire for privacy protections - for example, when lower privacy websites were put higher up on the search engine results list, users still chose to scroll down and select the higher-privacy protected site (Tsai, 2009). Therefore, this study demonstrated that privacy is a concern that consumers have, if they are aware about it and feel that they have the ability to control it. Therefore, if companies were to compete based off of privacy, it would add another crucial dimension of competition that the industry is overlooking right now, and consumers would exercise their choice based on many factors, privacy protection being one of them.

If there were to be competition on the amount of information and methods that companies employ to obtain user information, then companies would in effect protect consumer privacy because it would be another mode of competition among them. The consumers would then become the "regulators" in a sense because if a company was found to have lied or not disclosed

all their tracking practices, then consumers have the option of exercising their buying power and choose an alternative.

X. Policy Proposal

Consumers in the digital age have lost our buying power. The unit of currency has shifted from the physical dollar to information about the users, and because of industry standards and power, we are now trapped into giving away our privacy freely. This is happening because there are no viable alternatives for the user to obtain our products from companies that don't invade user privacy – in effect, the status quo is the assumption and practice that all companies can and will use user data whenever they want, with minimal governmental restrictions.

Since the real indicator of success in this growing information market is data about users, this should be the new "price" difference online – which company is less invasive on privacy of consumers. Once companies begin to vary in their privacy "prices", or the amount of data they collect from users and methods thereof, then competition will restore to the market and, in effect, this will reinstate the buying power back to the user, protecting their privacy in result.

Advertisements would still exist under this proposal, they just would be targeted to the consumer only if they themselves chose to give up their information to use the particular website. If the consumer chooses the option to not give up their personal data and to use that website, then there will still be advertisements – just not behavioral ones that were targeted, but rather generic ones comparable to the regular ads in newspapers or magazines – tailored to the topics of the website, but not to the particular consumer. This proposal would in no means stop the development or innovation of methods of advertising. Companies still have a need to monetize their content and directed advertisements certainly are very effective. Since advertisers pay more for behavioral advertising, perhaps these sites would generate more revenue and therefore provide better or more user-friendly content and services, which would entice some users to allow tracking. However, other websites would not track the user, and would either have less

revenue or attempt to make up the difference in different ways. Perhaps they would introduce a paid system, ask for user contributions in exchange for not tracking, or obtain investments from privacy-friendly organizations. These companies could even be spurred to develop another way to monetize content on the Internet that doesn't involve invasion of user privacy without their consent. This proposal simply advocates that that companies stop their anti-competitive practices of unrestrained methods of collection and introduce a level of competition that is currently absent from the discussions. If these companies do not take the affirmative action upon themselves to change their practices, the FTC could exercise it's soft power, publically release statements against these companies, or even threaten suit for anticompetitive behavior and monopolization in restraint of trade.

This proposal is not without possible supporters. Douglas Kysar "has claimed that consumers should have a right to make choices of products based on how the products are made, not just how well they work" (Pasquale, 2011). By letting the user make the choice about what information they will reveal and how it will be shared, the user is then not just informed of the current scenario, but also given the opportunity to structure what information they would like to give out to use the service. This proactive proposal mitigates the issues presented previously this paper. Academics or regulatory agencies would still need to check up on the companies to make sure that they are adhering to their prescribed policies, but there would be a much greater impetus for companies to make sure that they are providing the consumers with the correct information because the risk would be that consumers would leave their service due to the availability of alternatives. Therefore, circumvention of user choice would be addressed, and since the consumers would essentially be enforcing the market system, then companies would be forced to make users very aware of their privacy "prices" in order to attract consumers, in the

same way that companies display their monetary prices for goods. This proposal is not without its flaws, but it is intended to demonstrate the lack of ability of consumers to choose, and the lack of necessity of companies to constrain their behavior of tracking users in the current or even proposed systems by the Department of Commerce.

XI. Conclusion

The information asymmetry occurring between users, regulators, and the industry is apparent. The Department of Commerce's Codes of Conduct proposal and the Do Not Track proposal by privacy advocates attempt to address the issue of circumvention of user choice in their explicitly stated tracking preferences. However, these proposals are completely voluntary and reactive – they impose penalties on companies that do not comply with the provisions, but essentially require a "watchdog" of sorts to monitor companies' methods constantly. These proposals also could result in confusing users even more because they do not prevent all types of targeted advertisements. Because of the industry's desire for as much information as possible to more effectively advertise, and their past practices of subverting stated procedures and preferences to obtain user data, it is apparent that personal and behavioral information about users is very important to obtain for the industry.

These companies have and will continue to gather this information, and absent any proactive prohibition or real mechanism of regulation or enforcement, will continue to change their technologies to be able to continue competing in the marketplace and obtaining revenue. This is the organizational behavior that has persisted and will continue unless a proactive approach is taken. One proposal for this would be viewing personal information as the unit of commerce, thereby introducing the necessity of competition in the realm of privacy on the part of the companies. This would not prohibit directed advertisement or destroy the advertising business, but rather would result in a more effective market system, the restoration of consumer choice back into the equation, and ultimately leading to the securing of privacy. Undoubtedly, other alternatives exist and may be more effective. However, consumers are the harmed party in this system of collection of information, even though their data is the mechanism by which the

companies themselves are able to continue producing their services. This is an ironic occurrence, which should be examined further and changed to protect user choice and voice.

XII. Bibliography

Zuckerberg, Mark and Sheryl Sandberg. Exclusive Interview with Facebook Leadership: Mark Zuckerberg, CEO/Co-Founder & Sheryl Sandberg, COO Charlie Rose. 7 November 2011.

Zaneis, Mike. RE: tracking-ISSUE-93: Should 1st parties be able to degrade a user experience or charge money for content based on DNT? [Tracking Definitions and Compliance]. 20 October 2011. 20 April 2012 <http://lists.w3.org/Archives/Public/public-tracking/2011Oct/0158.html>.

Whittington, Jan and Chris Jay Hoofnagle. "Unpacking Privacy's Price." North Carolina Law Review (2012).

Angwin, Julia. Google in New Privacy Probes. 16 March 2012. 9 May 2012 <http://online.wsj.com/article/SB10001424052702304692804577283821586827892.html>.

Appari, Ajit, M. Eric Johnson and Denise L. Anthony. "The Neo-Institutional View of HIPAA Compliance in Home Health Care." Association of Information Systems SIGSEC (2009).

Backes, Michael, et al. ObliviAd: Provably secure and Practical Online Behavioral Advertising. Germany, 2012.

Barrett, Jennifer. "How Do Businesses Use Customer Inforamtion: Is the Customer's Privacy Protected?" Chief Privacy Officer, Axicom. Trade, and Consumer Protection Subcommittee on Commerce. 26 July 2001.

Beales, Howard. "The Value of Behavioral Targetin." Network Advertising Initiative, 2010.

Bilenko, Mikhail, Matthew Richardson and Janice Y. Tsai. Targeted, Not Tracked: Client-side Solutions for Privacy-Friendly Behavioral Advertising. Redmond, WA: Microsoft Corpoartion, 2011.

Bradley, Tony. "Do Not Track" Has It Backwards. 24 February 2012. 25 February 2012 <http://www.pcworld.com/businesscenter/article/250616/do_not_track_has_it_backwards.html#tk.mod_stln>.

—. Google Privacy Fiasco Lesson: There Is No Privacy. 20 February 2012. 10 March 2012 <http://www.pcworld.com/businesscenter/article/250328-2/google_privacy_fiasco_lesson_there_is_no_privacy.html>.

Brandeis, Louis D. and Samuel D. Warren. "The Right to Privacy." Harvard Law Review IV.5 (1890): 193-220.

Edelman, Ben. "Google Toolbar Tracks Browsing Even After Users Choose "Disable" ." 26 January 2010. www.benedelman.org. 28 November 2011 <http://www.benedelman.org/news/012610-1.html>.

Edelman, Lauren B. "Overlapping Fields and Constructed Legalities: The Endogeneity of Law." The Dynamics of Capital Market Governance: Evaluating the Conflicting and Conflating Roles of Compliance, Regulation, Ethics and Accountability. Canberra: Australian National University, 2007.

Edelman, Lauren. "Overlapping Fields and Constructed Legalities: The Endogeneity of Law." O'Brien, Justin. Private Equity, Corporate Governance, and the Dynamics of Capital Market Regulation. London: Imperial College Press, 2007. 55-90.

DiMaggio, Paul J. and Walter W. Powell. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." American Sociological Review 48 (1983): 147-160.

Federal Trade Comission. FTC Guide to the Antitrust Laws. 2012. 15 April 2012 <http://www.ftc.gov/bc/antitrust/antitrust_laws.shtm>.

—. Legal Resources - Statutes Relating to Both Missions. 2012. 15 April 2012 <http://www.ftc.gov/ogc/stat1.shtm>.

—. Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers. Washington, D.C.: United States Federal Trade Comission, 2012.

Fisher, Ken. Why Ad Blocking is devastating to the sites you love. 6 March 2010. 29 January 2012 <http://arstechnica.com/business/news/2010/03/why-ad-blocking-is-devastating-to-the-sites-you-love.ars>.

Google, Inc. Google Closes Acquisition of DoubleClick . 11 March 2008. 2 April 2012 <http://www.google.com/intl/en/press/pressrel/20080311_doubleclick.html>.

Gross, Grant. US Dept. of Commerce: New online privacy rules needed. 16 December 2010. 14 2012 April <http://www.networkworld.com/news/2010/121610-us-dept-of-commerce-new.html?page=2>.

—. Commerce Department Will Push Privacy Codes of Conduct. 21 July 2011. 2012 24 February <http://www.pcworld.com/businesscenter/article/236278/commerce_department_will_push_privacy_codes_of_conduct.html>.

Hoofnagle, Chris, et al. "How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?" Social Science Research Network. 14 April 2010.

Jaycox, Mark M. Facebook's (In)conspicuous Absence From the Do Not Track Discussions. 15 March 2012. 19 March 2012 <https://www.eff.org/deeplinks/2012/03/facebooks-inconspicuous-absence-do-not-track-discussions-when-individual>.

Kumari, Prachi. "Requirements Analysis for Privacy in Social Networks." 8th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods, 2010.

Lessig, Lawrence. Privacy as property - Part V: Democratic Process and Nonpublic Politics. 12 April 2002. 19 April 2012 <http://www.englishdiscourse.org/lessig.html>.

LinkedIn. LinkedIn Ads Campaign Pricing - Overview. 17 January 2012. 9 May 2012 <http://help.linkedin.com/app/answers/detail/a_id/7431>.

Nehf, J. P. "Shopping for Privacy on the Internet." Journal of Consumer affairs 41.2 (2007): 351-375.

Mayer, Jonathan. Do Not Track Is No Threat To Ad-Supported Businesses. 20 January 2011. 24 March 2012 <http://cyberlaw.stanford.edu/blog/2011/01/do-not-track-no-threat-ad-supported-businesses>.

Mayer, Jonathan R. and John C. Mitchell. "Third-Party Web Tracking: Policy and Technology." Stanford University, 2012.

Madrigal, Alexis. How Much Is Your Data Worth? Mmm, Somewhere Between Half a Cent and $1,200. 19 March 2012. 21 April 2012 <http://www.theatlantic.com/technology/archive/2012/03/how-much-is-your-data-worth-mmm-somewhere-between-half-a-cent-and-1-200/254730/>.

Misener, Paul. "How Do Businesses Use Customer Information: Is the Customer Protected?" Vice President Global Public Policy. Trade, and Consumer Protection Subcommittee on Commerce. Federal Trade Commission, 26 Jul 2001.

Purcell, Kristen, Joanna Brenner and Lee Ranie. 2012.

Pasquale III, Frank A. Dominant Search Engines: An Essential Cultural & Political Facility. 15 January 2011. 28 February 2012 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1762241>.

Pearson, Harriet. "How Do Businesses Use Customer Information: Is the Customer Protected?" Chief Privacy Officer, IBM. Trade, and Consumer Protection Subcommittee on Commerce. 26 July 2001.

Sutter, John D. Report: Pinterest is third most-visited social site. 9 April 2012. 13 April 2012 <http://edition.cnn.com/2012/04/06/tech/social-media/pinterest-third-social-network/index.html?eref=rss_latest&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+rss%2Fcnn_latest+%28RSS%3A+Most+Recent%29>.

Swire, Peter. "Privacy and Antitrust." Center for American Progress, 2008.

Scotchmer, Suzanne. "Competition Law and IP Law." UC Berkeley, 2011.

Selden, Larry and Geoffrey Colvin. Angel Customers and Demon Customers. The Penguin Group, 2003.

Soltani, Ashkan, et al. "Flash Cookies and Privacy." 2009.

Rule, James B. "The Whole World Is Watching." Democracy, A Journal of Ideas 22 (2011).

Rule, James. Privacy in Peril: How We are Sacrificing a Fundamental Right in Exchange for Security and Convenience. Cary: Oxford University Press, 2007.

Reitman, Rainey. White House, Google, and Other Advertising Companies Commit to Supporting Do Not Track. 23 February 2012. 10 March 2012 <https://www.eff.org/deeplinks/2012/02/white-house-google-and-other-advertising-companies-commit-supporting-do-not-track>.

—. April 2012, the State of Do Not Track: Lead Up to Tracking Protecting Working Group Negotiations in Washington, DC. 5 April 2012. 21 April 2012 <https://www.eff.org/deeplinks/2012/04/april-2012-state-do-not-track-lead-tracking-protecting-working-group-negotiations>.

Roosendaal, Arnold. "We Are All Connected to Facebook...by Facebook!" European Data Protection: In Good Health? (2012): pp. 3-19.

Turow, Joseph. The Daily You: How the Advertising Industry is Defining Your Identity and Net Worth. Yale University Press, 2011.

Temple, James. Chris Hoofnagle discusses online privacy. 21 August 2011. 5 April 2012 <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/08/20/BU5H1KP1HO.DTL>.

The Department of Commerce Internet Policy Task Force. Commercial Data Privacy And Innovation In The Internet Economy: A Dynamic Policy Framework. Washington, D.C.: United States Department of Commerce, 2010.

The Department of Commerce, Internet Policy Task Force. "Cybersecurity, Innovation and the internet Economy." 2011.

Tsai, Janice Y. The Impact of Salient Privacy Information on Decision-Making. Dissertation. Carnegie Mellon University. Pittsburg, 2009.