A Socialist Theory of Privacy in the Internet Age: An Interdisciplinary Analysis
Scott Confer

Abstract
In this essay, I examine the philosophical, political, and economic aspects of privacy in the Internet Age and argue that a socialist theory of privacy is the most suited for the contemporary privacy issues of the Internet. In section 2, I examine classic theories of privacy and argue that a Restricted Access/Limited Control theory offers the best framework and should be refined as a socialist theory of privacy. In section 3, I assess this theory in the context of the Internet Age, using Internet cookies and data mining as primary examples. In section 4, I describe the economic goals of a socialist theory of privacy and contrast them to liberal privacy notions. In Section 5, I review current and proposed privacy policies in the United States and give recommendations on revising them to support a socialist theory of privacy. In Section 6, I conclude that a socialist theory of privacy defines moral and economic goals that align with what is best for society as a whole and that, although our current policies are not working towards these goals, there is a glimmer of hope with the Consumer Privacy Bill of Rights.

1 Introduction
In the past, the biggest privacy concerns have stemmed from citizens wanting to hide certain information from their governments. This is still a major issue in modern society, but as the power of corporations has grown, the bigger issue of consumer privacy has emerged. The Internet Age, which enables greater and faster access to consumer information and sophisticated online tools for exploitation, compounds this issue. This allows corporations to conceal online practices from less technologically savvy consumers. Consumer privacy has reached the point where it must be addressed, but in order to do so there must be a clear definition of privacy and clear goals of what privacy should accomplish. Countless privacy theories have been proposed, many of which are outdated and do not apply to the Internet Age and others that misconstrue the purpose of privacy. In this paper, I argue that we should adopt a socialist theory of privacy and that our public policies should reflect this theory.

2 Examination of Theories of Privacy
Ferdinand Schoeman (1984) distinguishes among three categories of privacy definitions: (i) privacy as a claim, entitlement, or right; (ii) privacy as a measure of control over information, intimacies, or access; and (iii) privacy as a state or condition of limited access to a person. He argues that privacy as a right entails only that privacy is significant, not what is significant about it. Therefore, the right to privacy is not well defined. Any acceptable theory of privacy must include why a right to privacy is important. Similarly, defining privacy as a claim or entitlement simply states what privacy is, presuming the importance of it. Privacy as control over personal information has been countered by many with the example of a man on a deserted island. It is clear that he has lost all control over who has access to his information, but we would not say that he has no privacy. Unlike a claim or entitlement, this definition is not open to moral questions on the importance of privacy, but it is combated by many counterexamples. The last definition, privacy as a state or condition of limited access to information, intimacy, or thoughts, is what Schoeman argues is the best definition because it separates a loss of privacy from a violation of the right to privacy and leaves open the question of whether privacy is desirable. An example of a loss of privacy versus a right to privacy is when people willingly share their personal information. In this scenario, they clearly have a loss of privacy, but their right to privacy remains intact.

Schoeman's idea of defining privacy as limited access is broad, and it can be refined in many ways. One is a Restricted Access/Limited Control theory that is argued for by many theorists, including Herman Tavani. Tavani (2007) breaks down classic philosophical theories of privacy into slightly different categories
than Schoeman. These categories are: nonintrusion, seclusion, limitation, and control. Both nonintrusion and seclusion focus on physical access to individuals through observation. An invasion of privacy is defined in a physical sense, being physically intruded or having someone else physically in our presence. However, according to Tavini (2007), focus has shifted primarily to access over the control of personal information, often referred to as “informational privacy,” which is the emphasis of the control and limitation theories. These theories are more in line with the issues in the Internet Age as data access is not about physical invasions of privacy but rather where and how our personal information is accessed. Tavani argues that control theories, as the name suggests, often equate privacy to autonomy. According to control theories, someone could reveal everything about himself willingly and still maintain privacy because he maintains control and autonomy. In reality, this may not necessarily be the case. Limitation theories deal with whether the access to information is limited or not, but ignore where the control of access lies. Tavani argues that these limitation theories have the issue of confusing privacy with secrecy.

Ultimately, none of the four theories posed by Tavani are adequate in defining privacy. The control and limitation theories have the most merit, and both Tavani and Moor have argued that a combination of the two in a Restricted Access/Limited Control (RALC) theory provides the necessary framework for privacy. The key component stressed by Tavani is that RALC distinguishes between the condition of privacy and a right to privacy. In Schoeman’s categorization this makes RALC a definition of privacy as a state or condition of limited access. They share the similar goal of separating the right to privacy from the condition of privacy. Tavani outlines three important components of RALC:

1. Privacy is defined in terms of protection or limitation of access by others in the context of the situation.
2. An individual has normative privacy when there are explicit norms or laws protecting them.
3. Policies provide individuals with the limited control necessary to manage their privacy.

This theory holds two properties that I have deemed necessary thus far: it distinguishes between a violation of privacy and loss of privacy, and it addresses informational privacy issues. However, the requirements of a RALC are relatively broad and still beg many questions as to the specifics of these three components.

A more defined RALC theory, which I argue is the most justified, is proposed by Christian Fuchs in “Towards an alternative concept of privacy” (2011). His theory is founded on the basis that the liberal concepts of privacy are not desirable and that an alternative socialist conception of privacy should be explored. One of the most significant implications of his critique is that liberal privacy theories focus almost entirely on the positive aspects of privacy but ignore the negative ones. These negative effects include promoting individual agendas, allowing for misrepresentation of people’s character, and opposing participatory democracy. Fuchs gives an overview of the Marxian conception of privacy, and the primary conclusion is that the liberal concepts of privacy end in the alienation of humans from their social essence in the public sphere. Given both the positive and negative potential of privacy, the question a theory of privacy needs to answer is not how privacy can be best protected but rather in what situations privacy should be protected.

As argued by both Fuchs and Tavani, the context of a situation is key in determining how much to protect privacy. The socialist theory of privacy posed by Fuchs focuses on the distinction between classes in society, arguing that privacy should be used to strengthen the lower and middle classes, but it should not be used to protect corporations and the rich if this solidifies the gap between them and the lower classes. Ultimately, the socialist theory of privacy emphasizes both strengthening privacy for consumers and increasing transparency among capital owners. More generally, it advocates using privacy to protect the exploited from those exploiting them. This socialist theory uses privacy as a tool for leveling the playing field between an exploited group and a dominant one. For example, if a group X is being exploited by group Y, you increase the privacy of group X and increase the transparency of group Y until the exploited group is no longer being exploited. In reality, the big issue is then deciding how to accomplish this, but a socialist theory of privacy makes the ultimate goal clear given the current group dynamics. It can work with much more complicated situations as well. Say the exploited
group, group X, is actually dominating another group, group Z. You can increase group X’s transparency with respect to group Z, but not with respect to group Y, who is currently exploiting group X. The dynamics of any two groups is different, and a socialist theory of privacy reflects this. An important note is that this focus of a socialist theory of privacy is on groups, unlike liberal notions that focus on individuals’ privacy rights.

The robust socialist privacy framework can be applied to an issue between two consumers, two corporations, two racial groups, or any number of groups in society as long as one is exploiting the other. Because privacy issues in the Internet Age are primarily situations where consumers are left unprotected and corporations have the power to leverage this to their advantage, the main focus will be on consumers as the exploited group and corporations as the dominant group. If implemented into policy, a socialist theory of privacy provides the best framework to correct these exploitations, especially in the Internet Age.

3 Implications in the Internet Age

The Internet has brought unprecedented tools for monitoring and surveillance to the world. Helen Nissenbaum (2010) offers an enlightening anecdote about the difference between a day at the mall and an equivalent experience in cyberspace. In the physical world, you drive to the mall, browse through various stores, flip through some magazines, buy an ice cream with cash, and ultimately purchase a silk scarf with a credit card. The only real trace of you from this experience is your credit card payment. That is the only information that will be stored. In cyberspace, every action you make is a click. It is tracked and recorded: not only the magazines you looked at, the stores you entered, and what you browsed, but also how long you spent doing each activity. All this is recorded. This sort of monitoring throughout the Internet is made possible by cookies. The use of the information stored by cookies varies from website to website. The biggest use that will be discussed here is targeted marketing, in which cookies are used by media services to compile profiles based on individual interests and then show customized ads (Greenberg, 2003). The issue escalates when you enter personal information on a site that then stores a cookie on your computer which personally links you to an online profile that has been compiled on you.

For most people, a real issue arises only when personal information is tied to an online profile; however, I will argue that even without this tie to personal information, there is still a violation of privacy. The personal information just allows the issue to go beyond the cyber realm into other aspects of people’s lives. The first step for any RALC is to review the context of the situation. This begins with looking at the agents involved. In most cases, there is an individual consumer who is being monitored and profiled by a media service or company. It is also important to note that the user is often unaware of the information that is being tracked. Even though they have usually implicitly agreed to this, it is difficult to decipher what is actually being tracked without expertise. The situation can be summarized as a company taking advantage of a consumer’s lack of knowledge and using the information collected to increase profits. A socialist theory of privacy does not condone this action. In this situation, the consumer’s privacy is being violated rather than protected, and the actions of the companies responsible are rarely transparent due to the complexity of the tools being used. The main issue here is information asymmetry, the company knows more about what is being collected than the consumer. If this asymmetry were corrected by giving consumers a choice on whether or not they are tracked, then consumers would regain their privacy, and the actions of the companies would be transparent.

Data mining is another issue in the modern debate of Internet privacy. It is actually more related to cookies than many realize because cookies can provide the data for data mining. Although there are many definitions of data mining, here I will assume one of Florin Gorunescu’s (2011) definitions, “the automatic search of patterns in huge databases, using computational techniques from statistics, machine learning and pattern recognition” (pg. 4). Like cookies, data mining is not inherently meant to invade privacy. It even goes one step further than cookies and removes individuals from the equation, focusing on aggregates. However, detaching an individual’s identity from the data collected does not necessarily void the breach of privacy. Even in an aggregate, data mining still subdivides and categorizes individuals to breakdown trends. Consider a professor who analyzes the trend between students’ seats in the class and their grades. It is discovered that the back row averaged 20 points less on exams than the front row. Although no individual grades were released to the public, people will assume
that if you sat in the back row you got a worse grade. In this way, the patterns discovered by data mining trace correlations, not causation, and even if not explicitly stated like in the classroom example, the businesses that use data mining treat certain groups of people differently based on their findings.

One argument in favor of data mining, just like with Internet cookies, is that it may increase economic efficiency if firms know their consumers better. In reality, this information is not used to increase overall economic efficiency, rather it is used to increase the profits of firms at the expense of consumers. According to a socialist view of privacy, this is unacceptable because the context of the situation demands that consumers, who are vulnerable and exploited, must have their privacy protected. Firms have the ability to use data mining techniques and often conceal their findings, which results in similar issues of asymmetric information as with targeted marketing. Knowing nothing about these techniques, it is highly unlikely that consumers’ well-being will improve. Leaving them unprotected from these breaches of privacy allows firms to take advantage of consumers’ lack of knowledge.

There are countless other privacy issues that have arisen in the Internet age, including the seizing of cloud data, location tracking, and social media facial recognition. In these situations, the issues boil down to the same two points: consumers are not being protected well enough and firms are not transparent. The best way to correct these inequities is through a socialist privacy framework. To avoid reversing the exploitation, the framework must maintain a balance, ensuring that privacy is not increased too much and that firms are not forced to be too transparent. There is a point when increasing consumer privacy and increasing firm transparency has less benefit than cost on the public good, and at this point there is an equilibrium of privacy. This point has not been reached yet, and in the next sections I will examine the current political economy to assess how far away we are from this optimal level of privacy in the Internet Age.

4 The Economics of Socialist Privacy

The many liberal notions of privacy and the socialist one I suggest as an alternative begin to part ways greatly when discussing the economics of privacy. Richard Posner (1981) gives an argument on why concealment of personal information can be economically inefficient. He does so by classifying concealment of personal information as a form of fraud and attempts to counter opposing arguments to this concept. However, each counter argument holds true only with a liberal notion of privacy. When considered again in the context of a socialist theory of privacy, they do not always hold true. First, Posner rejects the idea that concealment of information is good because it provides a form of social insurance. He sees it as an inefficient form of insurance, where it shifts the costs from one group to another rather than distributing costs widely. However, the goal in a socialist theory of privacy is not necessarily to spread the costs widely, but to focus them more on capital owners in order to protect consumers. Although there may be a shift in where the costs are concentrated, if done correctly, it is more desirable than the original state where consumers are left bearing the costs.

Consider a recovering shopaholic, who built up a tremendous amount of credit card debt but has since learned to control his addiction. His past browsing data has been recorded by cookies, and it is possible that his personal information has been tied to it. Now as he is trying to recover, he is still exposed to targeted marketing ads on every webpage he visits for all kinds of things he used to buy, and he receives mail from local stores with deals for those products. In this unregulated environment, he may be drawn back into his old shopping habits, thus being exploited for profit by the corporations. Not only is this economically unjust, but also it poses a major ethical concern about firms forcing people into unhealthy habits, partially against their will. In this situation, concealment of the shopper’s past habits shifts the costs from him to the firms. Their potential profit is slightly less because they cannot exploit him, but he remains safely in recovery and improves his state of living. This concept of privacy as social insurance is desirable as long as the cost is shifted to the right place. The context is key, and if costs cannot be shifted to improve the overall well-being of society, then the information should not be protected. In this case, concealment improves both the overall economic state as well as an ethical one.

An overarching point that Posner (1981) makes is that arguments in favor of concealment of information can be “made with equal force by a seller asking for the right to conceal defects in his product, yet would be accorded scant consideration in that context” (pg. 406). This brings up the primary difference between a liberal notion of privacy and a socialist one. Under a liberal notion of privacy, Posner is correct and the argument
applies equally to a seller, but this ignores the important role that class plays in the context. In a socialist theory, a seller cannot make the same arguments because a seller is not equal to a consumer. Sellers should not be afforded the same protections if it will inevitably harm consumers.

There is a big distinction between liberal and socialist privacy and they have differing economic implications. The next aspect to examine is, in economic terms, when should a socialist theory of privacy protect information and when should it not? The goal of a socialist theory of privacy is to protect dominated and exploited groups from oppressors (Fuchs, 2011). This stands in contrast to liberal theories of privacy, which lack any distinct economic goal and rather argue for treating all individuals equally with regard to privacy, no matter their position in society. For most relevant situations in the Internet Age, the exploited group is consumers and the oppressors are corporations. In this specific situation, the economic goal is clear: to maximize consumer surplus. This should remain the goal as long as consumers are dominated by corporations, but if this were to shift in some way, then so would the context. In a general sense, the goal should be to maximize the well-being of the exploited group. Helping the exploited group may come at the cost of a decrease in total economic surplus, but maximizing surplus is not the economic goal of socialist privacy and so it is an acceptable consequence.

The economy is not naturally reaching the desired equilibrium of privacy in the Internet Age. As discussed in the preceding section, the issues arising from cookies and data mining are two examples of this disequilibrium. In fact, most issues of privacy on the Internet do not reach a level that adequately protects consumers. Privacy inadequacy is caused primarily by the market failure of asymmetric information, which is allowing corporations to be less transparent than they should be and leaves consumers less protected than they should be. Government intervention that helps strengthen the rights of consumers is needed to correct this. In the next section, I will examine some privacy laws in the United States and propose additional action as needed.

5 The Political Context of Socialist Privacy

There are countless policies effecting the wide range of issues that arise in Internet privacy. I will focus on the policies that have the most impact on data mining and Internet cookies since these are the issues with the largest considerations for socialist privacy and they represent a clear imbalance of power between consumers and corporations. We will start with current state-level policies to obtain an idea of what is missing in the legislation at the national level as well as how close the country is to adopting a policy nationally.

Pam Greenberg (2016) gives a comprehensive overview of the current state policies regarding Internet law. Two main sections of law are pertinent to consumer privacy on the Internet: personal information held by Internet service providers (ISPs) and privacy policies for websites. Only three states require websites to publicly disclose their privacy policies and only four states require ISPs to withhold personal information. In all other states, there are no explicit policies addressing these requirements. In some the requirements are non-existent and in others the requirements have fallen under policies unrelated to the Internet. Due to the amount, speed, and way in which data are acquired and the unique issues that arise, privacy on the Internet requires particular care and should have its own set of policies.

If the nation was to adopt the policies of this small minority of states, this would first require ISPs to get permission from their customers before releasing private information on them. In a sense, consumers maintain control of the data that their ISP collects on them. This policy would increase privacy for consumers, increase transparency for ISPs since their policy is explicitly stated in the law, and should ultimately lead to less exploitation. However, to achieve the goals of socialist privacy, these policies must also dictate how an ISP can use the information collected or, at the very least, that they must disclose this usage. This should prevent the ISP from engaging in any sort of exploitative behavior. Merely preventing them from sharing the data does not protect consumers from the ISPs. The second set of policies requires websites and online services to publicly disclose their privacy policies and those policies must not be false or misleading. This directly targets the issues of asymmetric information and company transparency that were identified as primary issues in Internet privacy. It shifts full control back to the consumers because it requires websites to tell consumers everything that will be done with their information. This policy does not allow companies to exploit consumers because consumers are aware of the websites’ policies. If implemented nationally, and if the policies are explicit and clear, this would be a huge step towards protecting the privacy of consumers and achieving the goal of a socialist theory of privacy.
These policies may not be a complete outline of what is necessary to fully protect the privacy of exploited groups, but they are more desirable than what is currently in place at the national level. Data policy at the national level is fragmented, and different privacy laws effect different industries (Kaal, Klosek, Waleski, 2012) making it difficult to decipher the true privacy rights of consumers. Privacy advocates have been pushing for a more unified national policy. A policy to fully protect consumers will need to be more comprehensive than what exists now.

One of the most notable attempts to overhaul consumer privacy and unify privacy policy at the national level is the Obama administration's Consumer Privacy Bill of Rights (CPBR) proposed in 2012. Although it is not currently enforceable, it provides a good idea on the direction that privacy policy is likely heading. The CPBR has seven principles for consumers' rights (Kaal, Klosek, Waleski, 2012):

1. To give individuals control over their personal data.
2. To have transparency about companies' privacy practices regarding consumers' personal data.
3. To give consumers the right to expect companies' use of data will be consistent with the context in which it was provided.
4. To ensure personal data will be secure and handled properly.
5. To give consumers access to the data that has been collected and allow them to ensure accuracy.
6. To provide reasonable limits on the personal data that can be collected.
7. To make companies' accountable for consumer's personal data.

This framework is more comprehensive than any single policy regarding Internet privacy that exists in the United States, thus it is already a step in the right direction. However, it is important to assess whether these seven principles are compatible with a socialist theory of privacy. The first two principles, control for consumers and transparency of companies, align perfectly with the socialist privacy goals defined previously. Consumers retaining control of their data is central to the socialist theory because it is the first step to becoming less exploited. The counterpart is corporate transparency which forces companies to share with consumers what data they are collecting and what is happening with that data. Both principals help tremendously in leveling the playing field between consumers and corporations.

The biggest question is what it means in principle 7, to provide “reasonable limits” on personal data that can be collected. According to Kall, Klosek, and Walkeski (2012), the CPBR allows companies to “collect personal data that they need to collect in order to accomplish the specific purpose for which the data was originally collected” (pg. 68). Although the condition is vague, it does give some assurance that companies cannot collect whatever data they wish. The concern is that companies still have full control over what they collect because they define the purpose of its original collection. It may be relatively easy to make an argument for why certain piece of data is needed even when it is not. This principle does not explicitly return control to the consumer because the potential for companies to collect more information than necessary still exists. There is also the question of what constitutes a valid reason for the original collection of data. One way to resolve this is to define standards, by industry, on allowed data collection. For example, online retailers may be allowed to collect browsing habits (with permission from consumers) to help improve the shopping experience, but it would seem irrelevant for a realtor to have this information even though it may help them find potential buyers. The key, again, is the context; in this case the type of firm must match the type of data collected. The CPBR is a big step in the right direction. If it were refined to return control to consumers and define what information should be collected, then it would fully work towards a socialist theory of privacy.

6 Conclusion

A socialist theory of privacy is the most desirable because it maintains the merits of a RALC theory, separating the right to privacy from the condition of privacy. In addition, it provides the best framework for improving privacy for those who need it most. The right to privacy is not necessarily a constant, and as context changes, so must the distribution of privacy. Given the current context of the world, the economic goal of privacy should be to maximize consumer surplus to the point where firms no longer exploit consumers. Politically,
with the current national policies in place, we are not even close to this point. There is promise, however, as some states enact laws pushing for increases in consumer privacy and firm transparency. In addition, the proposed Consumer Privacy Bill of Rights offers a set of principles that, if refined properly, could lead to a proper implementation of a socialist theory of privacy in the Internet Age.

Works Cited
Fuchs, C. (2011). Towards an alternative concept of privacy. Journal of Information, Communication & Ethics in Society

Gorunescu, F. (2011). Data Mining: Concepts, Models and Techniques: Springer Berlin Heidelberg.

Greenberg, E. A. (2003). What are cookies? Nursing, 33(6), 76-76. 9(4), 220-237.
Greenberg, P. (2016). STATE LAWS RELATED TO INTERNET PRIVACY. Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

Kaal, A., Klosek, J. & Waleski, B. (2013). U.S. Consumer Privacy Bill of Rights: Principles and Impact. Computer Law Review International, 13(3), pp. 65-72.

Nissenbaum, H. (2010). Privacy in Context. Stanford, California: Stanford University Press.

Posner, R. A. (1981). The Economics of Privacy. The American Economic Review, 71(2), 405-409.

Schoeman, F. (1984). Philosophical Dimensions of Privacy: An Anthology. Cambridge, MA: Cambridge University Press.

Tavani, H. T. (2007). PHILOSOPHICAL THEORIES OF PRIVACY: IMPLICATIONS FOR AN ADEQUATE ONLINE PRIVACY POLICY. Metaphilosophy, 38(1), 1-22.