Behavioral Advertising: tracking consumers with consent

Consideration of the substantive and procedural role of online contracts and other agreements, consent, and regulation of behavioral advertising in the US and the EU.

Candidate: Kevin D. McGillivray
Supervisor: Dr. Maryke S. Nuth
Deadline for submission: December/1/2010

Number of words: 17,736 (max. 18,000)
© 2010 Kevin D. McGillivray

http://www.duo.uio.no/ Trykk: Reprosentralen, Universitetet i Oslo
Abstract

Technologies have been introduced that allow companies to track consumer browsing online. Behavioral advertising, also referred to as behavioral targeting, is a method of collecting consumer information based on online behavior. From the information collected, by an advertiser, a detailed consumer profile can be created. The consumer profile is designed to provide advertisers with a more accurate picture of the kinds of services or products that a group of users, or a specific user, might be interested in purchasing. To better determine consumer preferences, tracking applications may record consumer purchases on a specific company’s website, or across multiple websites, including competitor’s websites.

The scope of the information collected, in many cases, is much broader than understood by the consumer. The legality of behavioral advertising and the use of tracking applications in the US and the EU often rest on consent provided by consumers. Disclosure of the applications, and the consent sought are generally facilitated by contract, privacy policies, term of use agreements, or end user agreements. Recent regulatory agency decisions in the EU and the US suggest that the consent provided by consumers may be questionable as terms and conditions of tracking applications are presented in a way that often makes them difficult for the consumer to understand or appreciate. This thesis will consider those concerns; discuss policy points raised, and provide a comparison of the regulatory systems in the US and the EU. The contracting methods and terms used to incorporate or facilitate these regulatory policies will also be considered.

1 Barnes, Wayne. RETHINKING SPYWARE: QUESTIONING THE PROPRIETY OF CONTRACTUAL CONSENT TO ONLINE SURVEILLANCE, 39 U.C. Davis L. Rev. 1545, 1547 (2006) (arguing that too little debate has taken place regarding a consumers right to consent to tracking applications which may have serious privacy consequences).
## Content

Abstract ....................................................................................................................... III  

1  Introduction ............................................................................................................. 1  
   1.1 Legal questions and problems considered .................................................... 2  
   1.2 Overview of chapters .................................................................................... 3  
   1.3 Legal method .................................................................................................. 3  
   1.4 Definitions and core concepts ....................................................................... 4  
      1.4.1 Electronic commerce .............................................................................. 4  
      1.4.2 Electronic contract ............................................................................... 5  
      1.4.3 Behavioral Advertising ........................................................................ 6  
      1.4.4 Privacy .................................................................................................. 7  

2  Online incorporation of Terms ........................................................................... 8  
   2.1 Introduction ..................................................................................................... 8  
   2.2 Online agreements: adaptations ................................................................... 9  
   2.3 Standard terms in online agreements ............................................................ 10  
   2.4 Presentation and disclosure of contract terms ............................................. 11  
      2.4.1 Browsewrap acceptance ....................................................................... 13  
      2.4.2 Clickwrap acceptance ......................................................................... 15  
   2.5 Browser settings as a means of providing consent ...................................... 17  
   2.6 Acceptance of online terms: consent .............................................................. 18  
      2.6.1 Privacy Policies .................................................................................... 20  
      2.6.2 End User License Agreements ............................................................... 21  
      2.6.3 Terms of Use Agreements (TOUs) ............................................................. 22  
   2.7 Presentation of BA terms, the case of Sears Inc. ........................................... 25  
   2.8 Limits to consent ............................................................................................ 28  

3  Behavioral advertising; law, regulation, and the role of contracts and consent .... 29  
   3.1 Overview and Scope ....................................................................................... 29  
   3.2 Behavioral advertising: background ............................................................... 29  
   3.3 Parties involved in behavioral advertising .................................................... 31  
   3.4 Profiling approaches ...................................................................................... 31  
   3.5 Scope of tracking technologies considered ................................................. 33  
   3.6 Cookies .......................................................................................................... 34
3.7 Deep Packet Inspection (DPI) technology........................................................................... 36
3.8 FTC and Working Party principles......................................................................................... 37
3.9 EU regulations .......................................................................................................................... 41
3.10 Opt-out v. Opt-in requirements............................................................................................... 44
3.11 Potential causes of action against behavioral advertisers: US ........................................... 45
  3.11.1 Right to privacy in the constitutional and common law....................................................... 45
  3.11.2 Statutorily based causes of action ..................................................................................... 46
  3.11.3 Causes of action based in tort............................................................................................ 49
3.12 Impact of behavioral advertising on online anonymity ....................................................... 49
3.13 Regulation: US and EU............................................................................................................ 50
4 Conclusion................................................................................................................................. 52
References...................................................................................................................................... 53
Literature......................................................................................................................................... 56
1 Introduction

Changes in technology have made a level of consumer surveillance possible that once only existed in science fiction. In the early days of the Internet, users had the ability to remain largely anonymous with their online browsing habits. This has changed. The adage of the 1990s, "nobody knows you are a dog on the Internet," no longer rings true. As stated by one commentator "[o]n the new targeted Internet, they now know what kind of dog you are, your favorite leash color, the last time you had fleas and the date you were neutered." The advent of new technologies, coupled with a reduction in the cost of online surveillance, has greatly increased the possibilities for data collection and identification of users online.

Consideration of the role played by behavioral advertising technologies in electronic commerce is important on both a practical and a normative level. From a practical standpoint, behavioral advertising has many economic benefits, including a means of funding for many startup web based companies. However, behavioral advertising may also have potentially negative implications for consumer privacy. On a normative level, exceptions in regulatory acts for consumer consent, provided by contract, make prohibitions or regulations of technologies difficult to enforce. The reality that consumers often waive substantial rights when they enter into contracts, or other agreements, is not a new concept. In the United States (US), consumers have long been able to bargain away substantial rights when accepting contract terms. For Americans, this includes their right to access local courts, the right to apply local law, and the flexibility to assume substantial risks, including bodily harm, when entering into a contract.

In the European Union (EU), the experience for consumers has been different. EU member states have generally subscribed to a higher level of consumer protection and legislated that

---


some rights are not derogable in consumer contracts. Nevertheless, consumers in the EU also face challenges to their privacy from behavioral advertising technologies. In this thesis I will consider some of the challenges posed by behavioral advertising and the role played by contracts and other agreements used to legitimize targeting practices. I will also consider the regulatory approaches taken in the US and the EU as they relate to behavioral advertising.

1.1 Legal questions and problems considered

I will consider legal questions regarding the role of contract terms, and other agreements, as the means of legitimizing behavioral advertising applications or practices. Specifically, I will consider whether terms, which state that a consumer consents to having behavioral advertising technologies installed on their computer are presented in manner that consumers are able to understand and consent to.

I will also compare the current systems in place to protect the privacy of consumers in the US and the EU. I will then consider this question from the view of both contract and data protection law. Further, I will discuss whether the systems in place provide sufficient consumer protection, either contractually or in regard to data protection, as the regulations relate to data collection via behavioral advertising technologies. I will also consider whether consumers have adequate causes of action for breaches of privacy rights, either by way of contract, or other statutory regulation. Specifically, what are the advantages of the remedies available in either the US or EU systems? The more direct question which will be considered is whether the US system of “self-regulation” provides consumers with adequate protections.

Contracts, and other agreements, as they relate to behavioral advertising applications, will be the central discussion point of this thesis. Whether consumer consent, obtained via electronic contract or other agreement provides a sufficient legal basis to support behavioral advertising will be discussed. Specifically, I will consider the role of contract terms, provided in standard form contracts, as they relate to privacy policies, end user license agreements, and terms of use policies.

---

6 See Directive 93/13/EEC (“Unfair Terms Directive”) (limiting waivers of consumer rights including a consumer's right to go to court). Note: Full citations to all directives are available in the "References" section Infra.
1.2 Overview of chapters

The first chapter of this thesis consists of an introduction to the topic, legal questions considered, and the definitions of the core concepts.

The second chapter will consider the online incorporation of contract terms and other agreements. One of the central issues in this work will be to determine notice and consent requirements for the validity of contracts supporting behavior advertising. In this chapter I will consider the presentation of contract terms to consumers and the method of notice provided. I will specifically consider the rights consumers waive when they are entering into contracts or other online agreements. Finally, the second chapter will consider a recent regulatory action in the US, the case of Sears Inc, and discuss the answers that case may provide.

The third chapter will consider behavioral advertising and the legal issues surrounding the technology. I will provide brief definitions of the technology and define the parties involved. I will also consider current regulation in the US and the EU as well as recent actions taken by regulators.

1.3 Legal method

The primarily focus of this thesis will be on regulation of behavioral advertising in the US and the EU. Therefore, I will consider available legislation governing behavioral advertising, largely from those jurisdictions. Cases, articles, and legal perspectives will be largely drawn from the US and the EU. Foundational information, as well as the current structure of electronic contracts in the EU and US, will be discussed. Examples from outside the US and the EU will be considered where relevant. Codes or principles of self-regulation for behavioral advertising will also be considered.\(^7\)

Additional focus will be placed on recent regulatory decisions in the US and the EU. Decisions in the US come largely from the Federal Trade Commission, a US regulatory

---

\(^7\) Network Advertising Initiative (NAI)(Providing voluntary standards for companies to follow)(http://www.networkadvertising.org/about/).
agency (hereinafter "FTC"). In the EU, decisions of the Article 29 Working Party (hereinafter “Working Party”) will be used for comparative purposes. The Working Party is made up of a board of representatives comprised of supervisory authorities designated by each member state. In the EU, contracts will also be evaluated through the lens of various directives, regulatory decisions, and court actions. In the US, I will discuss court actions, the United States Code (“U.S.C”), the Uniform Commercial Code (“U.C.C.”), and model laws. Existing consumer legislation will be considered as a point of comparison between the US and the EU.

1.4 Definitions and core concepts

The need for new electronic commerce regulations have left legislators and regulators with considerable challenges in creating usable definitions that are able to adapt to changes in technology. Definitions must be specific enough that they are relevant and applicable to the technical concepts they represent. However, they must also remain vague and flexible enough that they do not immediately become outdated. Therefore, drafters must attempt to "future proof" and create legal definitions that will not become immediately obsolete. Below are some definitions that are applicable to the core concepts discussed in this thesis.

1.4.1 Electronic commerce

I will specify when legislation provides a specific definition for electronic commerce, which is pertinent in a legislative act or directive. In the absence of a specific definition, I will use the more general definition of “[t]he practices of buying and selling goods and services through online consumer services on the Internet.” The use of electronic means to carry out essential contracting functions is a hallmark of electronic contracting. Electronic commerce

---

8 See *Infra* §1.4.3. "Behavioral advertising"

9 Directive on data protection 95/46/EC Art. 30(1)(hereinafter “DPD”).


11 Id. Discussing electronic data interchange (EDI), electronic mail (e-mail), electronic fund transfers as examples of electronic commerce systems.
is often used in a generic sense to describe a wide range of systems used to carry out transactions.\footnote{Pastukhov, Oleksandr. INTERNATIONAL TAXATION OF INCOME DERIVED FROM ELECTRONIC COMMERCE: CURRENT PROBLEMS AND POSSIBLE SOLUTIONS, Tech. L. 310, 313 (2006).}

### 1.4.2 Electronic contract

The term "electronic contract" does not have a standard or universal definition.\footnote{Nuth, Maryke Silalahi, Electronic commerce Contracting: The Effective Formation of Online Contracts. At 43-44 (Oslo 2010).} In legislation, the term is often defined for the purpose of a specific legal code or regulation. An inclusive definition defines an electronic contract as "...the common will of the parties to create a legal phenomenon that is made, produced or controlled by means of electronics."\footnote{Nuth, at 45. (emphasis added).} This definition is inclusive and properly lays out the common thread through most online contractual agreements, that is, their electronic character.

In the EU, there is no uniform definition for electronic contract.\footnote{HÖrnle, Riefa, The Changing Face of Electronic Consumer Contracts, LAW AND THE INTERNET. At 93 (2009).} Existing definitions are found in various instruments regulating electronic commerce, for example, the electronic commerce directive (hereinafter “ECD”).\footnote{Id.} In the EU, a “distance contract” has been defined as “...any contract concerning goods or services between a supplier and a consumer under an organized distance sales scheme run by the supplier, who, for the purposes of the contract, makes exclusive use of one or more means of distance communication up to and including the moment at which the contract is concluded.”\footnote{Directive 97/7/EC protection of consumers in respect of distance contracts (hereinafter “DSD”).} This definition is helpful. However, it is broad enough to include contracts that are not completed online or by electronic means.

A general US definition of electronic contract is “any type of contract formed in the course of electronic commerce by (1) the interaction of two or more individuals using electronic means, such as e-mail, (2) the interaction of an individual with an electronic agent, such as a computer program, or (3) the interaction of at least two electronic agents that are programmed...
to recognize the existence of a contract.”\textsuperscript{18} A definition may be dispositive as to whether a certain law is applicable. If that is the case, the definition will be provided.

\subsection{1.4.3 Behavioral Advertising}

Behavioral advertising utilizes tracking technologies that are constantly changing. Therefore, the terms require a definition that is flexible and future proof.\textsuperscript{19} The Working Party defines behavioral advertising as:

Advertising that is based on the observation of the behavior of individuals over time. Behavioral advertising seeks to study the characteristics of this behavior through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests.\textsuperscript{20}

The FTC is charged with consumer protection and regulating unfair commercial practices in the US, including those taking place online.\textsuperscript{21} Behavioral advertising is defined by the FTC as "[t]he tracking of a consumer's online activities over time, including the searches the consumer has conducted, the web pages visited, and the content viewed in order to deliver advertising targeted to the individual consumer's interests.”\textsuperscript{22} In available literature, the terms behavioral advertising and behavioral tracking are used in relation to the same objectives, namely, creating user profiles based on online browsing or use.\textsuperscript{23} In this article the term “behavioral advertising” is used as it is more consistent with recent enforcement decisions. Behavioral advertising incorporates the tracking and profiling systems utilized. In addition, it

\begin{itemize}
  \item[18] Black's Law Dictionary (9th ed. 2009).
  \item[19] Directive 2002/58/EC (hereinafter “ECD”) applies to websites but is not applicable to data messages, or emails, as electronic contracts.
\end{itemize}
also includes the monitory aspect, advertising dollars, which is the driving force behind the development and deployment of targeting technologies and profiling systems.

1.4.4 Privacy

In this article references will be made to privacy. Privacy is an amorphous concept that is difficult to define. In this work the term privacy will consider what has been deemed “informational privacy,” the individual’s right to control what is known about them. If a more specific definition is applicable, it will be noted in the applicable section.


2 Online incorporation of Terms

2.1 Introduction

In this chapter I will discuss incorporation of online contract terms as the concept relates to behavioral advertising. I will also consider how behavioral advertising terms are presented to consumers, methods of acceptance, and the role the terms play in providing legitimacy to behavioral advertising applications. Discussion regarding a consumer's opportunity to review terms, disclosure of terms, and standard of notice will also be considered. This will require a comparison of various methods of online acceptance including, “clickwrap” and “browsewrap,” agreements.

The legal validity of behavioral advertising applications is often predicated on consent. Therefore, before behavioral advertising technologies can be lawfully deployed, consent must be obtained from the consumer. Behavioral advertisers often use the terms of online contracts, privacy policies, terms of use agreements, or end user license agreements as the method of presenting the terms. Whether they realize it or not, when consumers click a button, download a program, or browse a website, they may assent to terms in the agreement and provide the requisite consent for the tracking of their online activity.

In this chapter, I will also discuss the incorporation of terms and the general system of online contracting. First, I will consider the presentation of online agreements as standard term contracts. This will include a discussion of both the bargaining process involved and the methods of presentation. Second, I will discuss the common methods wherein behavioral advertisers incorporate terms, namely, privacy policies, term of use agreements, or end user

27 Id. As opposed to spyware, which is deployed without consent.
28 Wilson, Emma, DOUGLAS v. TALK AMERICA: MAKING THE CASE FOR PROPER NOTICE, 45 Idaho L. Rev. 479, 496 (2009). However, “…it is not enough that the terms can be found somewhere; the terms also must be presented in such a way that they can be found by the reasonable user.” Hartzog, at 406 (2010).
agreements. Third, I will demonstrate the concepts of contracting discussed in this chapter using a recent case from the US as an example.

2.2 Online agreements: adaptations

Consumers and non-professional parties enter into electronic contracts and other agreements on a daily basis.\textsuperscript{29} In the US, the active number of home Internet users is over 148 million.\textsuperscript{30} In Europe, the amount has been estimated at over 170 million.\textsuperscript{31} As a result of increased consumer Internet usage, a greater number of business-to-consumer (B2C) transactions are taking place in addition to the more traditional business-to-business (B2B) transactions.\textsuperscript{32} The substantial increase in B2C contracts online has resulted in the weaker party, consumers, bargaining and conducting business on an international stage. Therefore, in an attempt to provide adequate protections for the weaker party, legislative action has been taken in the EU to protect consumers. The EU directives currently in place to protect consumers include the Unfair Terms Directive the Misleading and Comparative advertising Directive, and the Unfair Commercial Practices Directive.\textsuperscript{33} In the US, the Uniform Computer Information Transaction Act (UCITA) provides a remedy for unfair terms, as they relate to transactions in computer information.\textsuperscript{34} However, the UCITA has only been adopted in two US jurisdictions; therefore, its application is limited.

\textsuperscript{30} Andrew Hotaling, PROTECTING PERSONALLY IDENTIFYING INFORMATION ON THE INTERNET: NOTICE AND CONSENT IN THE AGE OF BEHAVIORAL ADVERTISING, 16 COMMLAW CONSPECTUS 529, 529 (2008).
\textsuperscript{32} Id. A greater number of consumer-to-consumer (C2C) transactions are also taking place.
\textsuperscript{33} 93/13/EEC; 97/55/EC; 2005/29/EC; respectively. A directive 2008/0196, on consumer rights, is forthcoming.
\textsuperscript{34} UCITA §111 (2002).
2.3 Standard terms in online agreements

In the US, consumers entering into online contracts or other agreements are often presented with standard terms on a “take-it-or-leave-it-basis.” Standard term contracts do not allow consumers to negotiate terms they may not agree with. If consumers wish to purchase a product or utilize a service, they must accept the terms presented to them as a whole. It has been estimated that 99% of contractual agreements governing consumer purchases are presented in standard form. Although standard form contracts are often criticized by consumer rights advocates based on the one-sided character of the agreements, from a commercial perspective, they are often considered essential. If all contracts required individual negotiation, the speed of contracting would decrease while the cost of contracting would substantially increase. It is therefore clear that standard form contracting is not going away in the online age.

As a result of digital technology, an exhaustive list of terms can be provided to a consumer at very little expense. However, consumer protection remains an important issue, regardless of any real or perceived economic inefficacy it may present. For most consumers, the proposition of refusing to enter into a standard term agreement is unrealistic. Doing so may limit consumer access to modern necessities like credit cards, banking, and communications services. While the number of agreements consumers enter into continues to rise, the risks associated with “blindly accepting” online privacy notices or contract terms have also

36 Gindin, Susan E., at 36 (2009).
37 Definition of “consumer” is not uniform in the EU. See 97/7/EC Art. 2(a), 93/13/EC Art. 2(b). See also 97/7/EC Art. 2(a).
38 Wilson, Emma, at 483-84 (2009).
39 Restatement (Second) of Contracts § 211 cmt. a. (1979).
40 Id.
42 Pursuant to ECD 2002/58/EC Art. 10(2), the directive is applicable to contracts not formed by individual negotiation.
increased.\textsuperscript{43} Contract terms presented are often “long, detailed, full of legal jargon, about remote risks, and one-sided.”\textsuperscript{44} Online contract terms may also require that a consumer waive substantial privacy rights, agree to restrictive terms of use, and acquiesce to licensing terms presented by a third-party.\textsuperscript{45} Furthermore, the rights waived by a consumer may vary considerably, depending on the agreement. What is allowed or will be enforceable in a standard agreement also varies between the EU and the US.\textsuperscript{46}

It is, therefore, important for the consumer to consider the substance of the contractual terms being presented before agreeing to them. In the next section, I will discuss how the substance of the terms are often disclosed or presented to consumers. An examination of the varied methods by which terms are disclosed provides some explanation as to why consumers are willing to enter into what are arguably such one-side agreements.

\section*{2.4 Presentation and disclosure of contract terms}

As stated in the previous section, the substantive terms of the agreements consumers enter into are often on a standard form basis. Although the terms of the agreement may be standard, the methods of presenting and disclosing the terms to the consumer vary depending on jurisdiction and agreement type. Further, I will also explore some of the reasons terms presented in online contracts are difficult for consumers to understand or appreciate. I will also discuss the different approaches taken in the US and the EU in accepting contractual terms, and how they relate to behavioral advertising.

General contract principles require that before contractual terms may be imposed, they must be incorporated into the document.\textsuperscript{47} Legal systems in both the EU and the US have made

\begin{flushleft}
\textsuperscript{43} Gindin, Susan E., at 13 (2009).
\textsuperscript{44} Id.
\textsuperscript{45} Id.
\textsuperscript{46} Winn and Webber, at 228 (2006)(\textit{Maintaining} that “U.S. Internet businesses that target consumers in Europe need to be aware that standard form contracts that work well in the U.S. may be unenforceable in the EU.”).
\textsuperscript{47} HÖrnle, Riefa, at 109 (2010).
\end{flushleft}
accommodations for electronic contracting. However, business practices and legal standards continue to vary considerably between the US and the EU. Traditionally, by signing a document, a consumer was bound by the terms contained therein. In the US, the law “presupposes a consumer's duty to read all terms in a contract, with the concomitant effect that the consumer is thereby bound by such terms.” As a result, terms provided in an agreement allowing for behavioral advertising are generally valid, absent surprise or level of unfairness wherein they are declared void for public policy reasons.

In the online context what has been presented to a consumer, or should be considered part of the agreement, is not always clear. Online terms are often presented in a manner that requires the consumer to look outside of the immediate agreement in order to determine all the terms they are accepting or which are included in the agreement. A consumer entering into an electronic contract may be required to visit multiple websites of follow multiple links in order to determine what terms are applicable to the agreement. The presentation of online terms often makes it difficult for the consumer to review them prior to entering into an agreement and accepting them.

What constitutes a proper or legal presentation of contract terms online may vary by jurisdiction.

In addition to entering an agreement by online signature, there are several methods for electronic acceptance including "browsewrap", "web-wrap", and "clickwrap." The US and the EU have taken different approaches in accepting or rejecting these methods. Below the methods of accepting terms and entering into contracts will be considered.

---


49 Restatement (Second) of Contracts § 211(3) (emphasis added). Barnes, TOWARD A FAIRER MODEL OF CONSUMER ASSENT TO STANDARD FORM CONTRACTS: IN DEFENSE OF RESTATEMENT SECTION 211(3), 82 WASH. L. REV. 227, 228 (2007).


51 Id.

52 See e.g. Grierson, 106 A.L.R.5th 309 § 2(a) (2003).

53 Hörnle, Riefa at 110 (2009).


2.4.1 Browsewrap acceptance

In the "browsewrap" method of acceptance, contract terms are provided to a consumer on a webpage, which is generally accessible by hyperlink.\(^{54}\) Browsewrap agreements often provide that “any additional browsing past the homepage constitutes acceptance of proposed terms located on the Web site.”\(^{55}\) Although the terms are available if the consumer wishes to access them, there is no requirement that the consumer takes an affirmative step signifying that she has read the agreement.\(^{56}\) If the terms are displayed before the consumer assents to the agreement, they may be binding depending on the jurisdiction. Assent may vary by circumstance, but might include downloading software, purchasing a product, or even viewing a webpage.\(^{57}\) In the case of behavioral advertising, the terms applicable to the tracking application may be presented as part of a separate privacy policy, which is available by browsewrap or web-wrap before the agreement is completed, but is not included as a term in the central or “clickwrap” contract. The consumer may read the privacy policy if they wish, but they are not generally required to do so in order to access the service or purchase the product. However, to bind the consumer, some notice must be provided, as “a party cannot assent to terms he has no reason to know exist.”\(^{58}\)

In the EU, it has been deemed an unlikely prospect that simply browsing a website provides reasonable notice of contract terms.\(^{59}\) Therefore, consumer contracts presented by the browsewrap method will not generally be enforceable in the EU. In the US, Courts have taken different approaches in determining whether these agreements are enforceable.\(^{60}\) Although browsewrap terms have received some acceptance in the US, courts have been somewhat inconsistent their application in practice. In the cases that follow, it is clear that US

---

\(^{54}\) Specht v. Netscape Communications Corp., 306 F.3d 17, 29-30 (2d Cir. 2002).


\(^{56}\) Id.

\(^{57}\) Wilson, at 491 (2010).

\(^{58}\) Id. at 492 (2010) (Quoting Douglas, 495 F.3d 1062, 1066 (9th Cir. 2007)).

\(^{59}\) HÖrnle, Riefa at 110 (2009).

\(^{60}\) Kunz, Christina L. et al., BROWSEWRAP AGREEMENTS: VALIDITY OF IMPLIED ASSENT IN ELECTRONIC FORM AGREEMENTS, 59 Bus. Law. 279, 304-05 (2003).
courts place more weight on whether notice was provided before acceptance, rather than the method of display. As such, browsewrap terms will not always fail as a method of procurement.

In the case of Williams v. America Online, Inc., the US court determined that a forum selection clause was not applicable in the agreement because assent to the terms was required only after a consumer downloaded the product. In Williams, the consumer did not have the ability to consider or review the document until after the agreement had been accepted. As a result, the court deemed that the agreement was not enforceable against the consumer. The opportunity to review a document before being bound and provide “some manifestation of assent,” as well as the ability to stop the agreement if the consumer does not agree, are central aspects of a valid browsewrap agreement. In the leading US case on the matter, Specht v. Netscape Communications Corp., the Court applied similar logic to that in the Williams case and stated that "a consumer's clicking on a download button does not communicate assent to contractual terms, if the offer did not make clear to the consumer that clicking on the download button would signify assent to those terms." In that case, the end user license agreement (EULA) was not available to the consumer until after the download had been completed, thus, it provided no opportunity for review. The Specht Court provided that the “bare act of downloading the software did not unambiguously manifest assent to the arbitration provision contained in the license terms.” In its decision, the Specht Court determined that "reasonable notice of the license terms" was not provided.

---

62 Id.
63 Oakley, at 1054 (2010).
65 306 F.3d 17 (2d Cir. 2002).
66 Id. at 40.
67 Id. at 29. Stating that "[m]utual manifestation of assent, whether by written or spoken word or by conduct, is touchstone of contract."
However, in another US case, *Register.com v. Verio, Inc.*, a different result was reached by a federal district Court.\(^{68}\) In that case, the *Verio* Court held where terms were clearly posted on a website, they were enforceable against a user even if the user *never* affirmatively clicked on an “I accept button.”\(^{69}\) Similarly, in the case of *Ticketmaster Corp v. Tickets.com*, notice provided on a webpage was sufficient to bind a consumer to the terms presented, even without an affirmative act of agreement on behalf of the consumer.\(^{70}\) In the US, when considering enforceability of terms, courts put the greatest weight on the opportunity of the consumer has to review the terms before entering the agreement rather than the method by which the terms are delivered. Although there certainly may be some connection, that is, some methods of presentation make it easier for consumers to review the substance of the terms governing the agreement.

As demonstrated by the above case law, terms on a website which a consumer may not have affirmatively agreed to, may still be binding.\(^{71}\) In the case of browsewrap agreements, US courts seem to be willing to accept that notice has been sufficiently given where the terms, or the ability to access the terms is present. In the behavioral advertising context, agreements presented by Browsewrap will generally be considered binding in the US, as long as the information regarding the application is provided prior to consumer acceptance.

### 2.4.2 Clickwrap acceptance

Clickwrap agreements are often considered to be the best method of providing notice to consumers and creating binding contracts.\(^{72}\) As the draft of the ALI Principles of the Law of Software Contracts suggests, a fair assessment of the cases is that a click-through interface is a *safe harbor* of enforceability beyond which websites stray at their own peril.\(^{73}\) With “clickwrap technology” contract terms are presented to the consumer, and she must take an

\(^{68}\) 126 F. Supp. 2d 238, 248 (S.D.N.Y. 2000).

\(^{69}\) Id.


\(^{72}\) Id. at 993.

\(^{73}\) Mann, at 993 (2008).
affirmative step to accept the terms in order to complete a transaction. The assent provided generally requires that the user click a button or check a box stating "I accept" or "I agree."74 The systems used to present clickwrap terms are not uniform, but generally display terms in a "frame through which a user must scroll to get to a radio button that must be checked to proceed."75 In some cases, the presentation may include "terms within a frame and a radio button outside and below that frame that must be checked to proceed."76 The notice provided, not the design or display of the clickwrap window, is dispositive. The common distinction between the various contracting methods has been the affirmative action the clickwrap method requires from the consumer.77

Although affirmative action must be taken to complete the agreement, a consumer is not required to actually read the terms and conditions. In fact, it is very likely that consumers will not read the agreement. In a recent study, an author compared 58 cases where clickwrap agreements were litigated. The author concluded that “[a]lthough there are legitimate reasons for believing that computer users do not truly agree when clicking through electronic license agreements, invalidating all of these terms for lack of assent would have significant negative effects on electronic commerce.”78 Therefore, the opportunity to review the agreement provides the distinction and provides courts with at least the appearance of contractual fairness. The inclusion of numerous legal terms into electronic contracts has not been without criticism. Some of the most controversial inclusions have been terms “forbidding public criticism of the product, requiring consent to third-party monitoring, prohibiting reverse engineering, prohibiting use in connection with third-party software, requiring consent to future revisions of the agreement (which is subject to change without notice), disclaiming warranties, and disclaiming liabilities.”79

74 See e.g. Moore v. Microsoft Corp., 741 N.Y.S 2d 91 (2002).
76 Id.
77 Mann and Siebeneicher, at 984 (2008).
78 Id. at 998.
In the US, courts have considered and upheld clickwrap agreements since the 1990s. American courts have generally held that the presentation of terms provides the consumer with reasonable notice. Regardless of what often appears to be a judicial endorsement of clickwrap, some courts have been less willing to accept clickwrap agreements. Although the substances of the terms delivered via “clickwrap” have been successfully challenged, the method of delivery is generally considered to be legally sound. For example, in the State of New York, a court refused to enforce a forum-selection clause entered into by clickwrap license. However, the New York Court’s decision to invalidate the agreement was based on its determination that the terms of the agreement were in violation of state public policy rather than a deficiency in the clickwrap method of delivery.

### 2.5 Browser settings as a means of providing consent

The Internet continues to challenge the way we apply traditional legal terms like acceptance or consent. When consumers visit web pages websites will often request to install “cookies,” on the consumer’s browser. Consumers have the ability to pre-set their Internet browser to accept or reject the installation of cookies on their computers. If the browser is set to “accept all cookies,” which is the default setting of all major Internet browsers, acceptance of cookies takes place automatically. As a result, “a different class of consent has emerged…where the action underlying the alleged consent is taken not by a human but by a computer.”

The practice of browser led acceptance has been generally accepted in the US. Default acceptance of cookies is currently the general business practice in the EU. Until recently, default acceptance, expressed in browser settings, was thought to be consistent with the directive on privacy and electronic communications 2002/58 (hereinafter “ePrivacy”)

---


81 CompuServe, 89 F.3d at. 1260-61. See also Alces and Greenfield, at ¶ 1102-06 (2010).


83 Id.

84 “Cookies” discussed Infra at § 3.6.

85 Oppenheimer, at 9 (2010).

86 Eecke et al., RECENT EVENTS IN EU INTERNET LAW—EUROPE.14 No. 3 Internet L. 25, 25 (2010).
However, a regulatory opinion by the Working Party suggests that this practice does not obtain proper consent, pursuant to EU law. The Working Party contends that, pursuant to Article 2(h) of Directive 95/46/EC, consent provided as a default browser setting will not be considered valid. As has been noted by the Working Party “[a]verage data subjects are not aware of the tracking of their online behavior, the purposes of the tracking, etc.” As a result, the browser method of consent undertaken solely by a computer may be short-lived in the EU. In the US, it has not been problematic for the purposes of accepting cookies, which may be used for behavioral advertising purposes.

2.6 Acceptance of online terms: consent

In the previous sections the various methods of presenting terms for review by consumers were considered. In this section, I will consider some of the standard types of agreements governing privacy terms. I will also discuss the agreements and consider how they are presented.

A core question that must be addressed in the presentation of the terms is whether the terms actually provide consumers with enough information that the consumer is able to provide consent. Consent falls into two general categories. “If it is clearly and un-mistakably stated, it is referred to as express consent, while if it must be inferred from conduct, it is referred to as implied consent.” Therefore, for consent to be valid, affirmative action is not always necessary. In some circumstances, silence may be appropriate. Although courts

88 Id. Eecke et al., at 25 (2010)(Providing certain conditions that must be met for acceptance by browser settings).
90 Id. Noting that out of the four major publicly used browsers, only one allows users to block third-party cookies.
91 Discussed Infra § 3.
92 Consent is most generally defined as “[a]greement, approval, or permission as to some act or purpose.” Black’s Law Dictionary, at 323 (8th ed. 2004).
93 Oppenheimer, at 9 (2010). See DPD 95/46 Art. 2(h). Consent “shall mean any freely given specific and informed indication…” See also DPD 95/46 Art. 8(2)(Defining “explicit consent”).
94 Id.
and legislators generally seem to favor the presentation of terms in the clickwrap variety, as we have seen through case law, at least in the US, the method used to present the terms is not necessarily dispositive. To be valid, "[c]onsent requires a knowing understanding of what one is doing in a context in which it is actually possible for one to do otherwise, and an affirmative action in doing something, rather than a merely passive acquiescence in accepting something."96

Therefore, it has been noted that "[a] well-advised website designer would require some affirmative action from the user, indicative of assent to the document in question, in order to reliably produce a binding contract."97 Acceptance or authorization can take place as an action and formalities are not required.98 As a general rule in American jurisprudence, the cases where courts will most likely refuse to enforce a contract in favor of a business are those “where the user was not required to assent to the terms or was asked to consent to the terms only after he downloaded the product.”99 Therefore, businesses that fail to present terms to consumers before an agreement takes place, or change terms after an agreement is finished, run the risk of having those terms held unenforceable.

Due to the shape of modern agreements, it is often difficult to present terms in this regard. Many agreements consumers enter into are with multiple parties, which may each have their own terms and privacy policies. It is therefore often difficult to determine what the terms are, if a privacy policy has changed, or exactly what the terms require. In the following sections of this chapter, I will consider some of these agreements individually, and discuss their impact on consent.

95 Id.

96 Margaret Jane Radin, HUMANS, COMPUTERS, AND BINDING COMMITMENT, 75 Ind. L.J. 1126 (1999); See also Oakley, at 1065 (2005).

97 Mann and Siebeneicher, at 984 (2008).

98 Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 403 (2d Cir. 2004).

2.6.1 Privacy Policies

The breadth of privacy a consumer waives when using a website is not always clear to the user. Like contracts, privacy policies are often written in a "standard" form and do not provide consumers with an opportunity to negotiate individual terms. For consumers, it is not always clear what the policy includes, particularly when the consumer is dealing with multiple parties. Unlike many contractual agreements, privacy policies often do not require that a customer “click-through” or assent to specific terms. As a result, consumers may not be actively put on notice of the terms of an agreement. If visiting a website, or use of an online service requires the assent to multiple privacy policies, it may be difficult for a consumer to locate all of the agreements. For example, a consumer may agree to the privacy policy of a website publisher, and in doing so, be subject to the privacy policies of ad services displayed on the website and terms of third-party software providers. Many privacy experts assert that complex privacy policies contained in a single document do not provide effective information regarding privacy practices. Finding the statements, combining the terms, and understanding their implications are an onerous task for consumers.

Although privacy policies may impact consumers in much the same way they are impacted by contract terms, presentation of the policies often fails to meet standards, which are generally considered acceptable in online contracting. The contracting method of presenting terms to the consumer, and then requiring affirmative acceptance, is not always followed. For example, privacy policies often contain terms that allow the company to change user data standards at anytime and do not required additional notice or consumer consent. Web site privacy policies often utilize “browsewrap” technology, require that the consumer find


102 Id.


104 Id. at 552.

105 See § 3.2 *Supra* discussing formation.

applicable terms and conditions on another webpage, and do not require affirmative confirmation, or "clickwrap" assent of privacy terms by a consumer.\textsuperscript{107}

For many companies, it is preferable to keep the privacy policy outside of the contractual agreement.\textsuperscript{108} As noted in one study, “[t]he retailer gains little or nothing from making a privacy policy binding, because the typical privacy policy consists solely of representations and commitments by the retailer as to the collection, use, and protection of information.”\textsuperscript{109}

From the prospective of legal risk management, by presenting a privacy policy separately, and keeping it outside of the contractual agreement has certain advantages for a behavioral advertisers or publishers.\textsuperscript{110} If the terms of the agreement are not contractual, the business is not bound by the agreement, thus it retains a greater level of flexibility to later make changes to terms without seeking consent from the consumer. Furthermore, potential liability may also be limited as a “breach of contract” action based on the privacy policy as a contract between the parties, will be unavailable to the consumer.\textsuperscript{111}

\textbf{2.6.2 End User License Agreements}

End user license agreements (EULAs) are often presented to consumers making online purchases. The agreements are often presented as a means of protecting the intellectual property rights of a third-party. The EULA process is often as follows:

A buyer purchases software in a shrink-wrapped box or--as is now routine--by downloading it online; a standard form contract is inside the box (a shrink-wrap EULA) or displayed on a splash screen during installation (a clickwrap EULA). No negotiation is allowed; by the time the buyer can read the agreement the only options are to return the software or accept the terms. When return is not a meaningful option, acquiescence is the only alternative.\textsuperscript{112}

\begin{itemize}
  \item \textsuperscript{107} Id.
  \item \textsuperscript{108} Mann, at 984 (2008).
  \item \textsuperscript{109} Id. at 1001.
  \item \textsuperscript{110} Id. Maintaining that “there is some authority for the proposition that a retailer is not subject to suit by its customers [in the US] even if it does violate the terms of its privacy policy.”
  \item \textsuperscript{111} Id.
  \item \textsuperscript{112} Warner, Richard, TURNED ON ITS HEAD?: NORMS, FREEDOM, AND ACCEPTABLE TERMS IN INTERNET CONTRACTING., 15 No.5 Internet L. 18, 18 (2010).
\end{itemize}
In this situation, buyers have very little bargaining power to oppose terms they may deem unfair. Patients have upheld the EULA practice as applicable in B2C transactions. In the US, EULAs are often considered to be more “pro-seller” than the rules applicable by default pursuant to the Uniform Commercial Code. If multiple parties are involved, it can be difficult for a consumer to determine which party they are entering into an agreement with. Consumer advocates often argue that EULAs do not provide consumers with proper notice of terms governing the agreement.

2.6.3 Terms of Use Agreements (TOUs)

In addition to the terms presented in the contract, and agreements governing interactions with third-parties, consumers may be bound with additional terms. Terms of use agreements (hereinafter “TOU agreements” or “TOUs”) are agreements governing the use of websites or web-based services. TOU agreements are often presented on a browsewrap rather than a clickwrap basis. TOUs are available primarily on a passive basis and do not require affirmative assent by the consumer in accepting the terms.

To determine the rules applicable in a TOU agreement, the consumer is often required to follow hyperlinks to another website where the rules governing use are provided. As a result of the myriad of steps for the consumer, TOUs agreements are rarely read. As noted by one commentator “[w]eb site owners may--and do--exploit this fact to impose terms that unacceptably compromise a visitor’s privacy.” TOUs agreements often contain provisions, which provide the necessary authorization for allowing businesses to collect information from

113 Id. at 19.
114 e.g. ProCD v. Zeidenberg, 86 F.3d 1447 (7th Cir.1996).
116 Id. at 18 (2010).
117 Id.
118 Id.
119 Id.
120 Id. at 19. (Maintaining that TOUs pose the most significant challenge to current contract law).
visitors. Traditionally, TOU agreements have been deemed an acceptable means to justify the collection of consumer data by US courts.

In the past, US courts have provided some acceptance of allowing companies to change or shift privacy policies. The test applied has generally been that of the Specht Court, discussed Supra. Namely, if a consumer has a reasonable opportunity to inspect terms, the terms may potentially bind the user. However, some recent decisions have added some question marks around the TOU practice. In Harris v. Blockbuster Inc, the Court refused to uphold a TOU agreement, which was presented in clickwrap format, that allowed the company “at its sole discretion and at any time” to modify the terms of the agreement. The Harris Court held the terms of the contract, which in essence only bound the consumer, were illusory and unenforceable. This case shows that some unilateral terms will not be acceptable, even in the US where consumers are given wide latitude in accepting terms. In the US there is a requirement of consideration, or a bargained for exchange, which requires parties to exchange a benefit for a detriment when forming a contract. If only one party is bound by the terms, this requirement will not be met. Another issue in Harris is the right at stake. In that case, the terms shifted were not in regards to a behavioral advertising policy. Rather, they concerned certain consumer rights for adjudication of claims in a court. Furthermore, the decision was by a federal district court, which is subject to appeal in an appeals court.

In the previous section I discussed the different types of agreements wherein privacy policies are presented. As noted in each section, agreements providing the legal basis for behavioral advertising policies, which do not require affirmative consent, have been widely accepted by courts. In this section, I will discuss specific regulatory efforts taken to police the agreements.

121 Id. at 28.
125 Id.
127 Id.
In the US, a consumer wishing to void, or defend themselves against enforcement of an agreement may assert several defenses including the doctrine of unconscionability or argue that the contract is illusory or based on surprise contract terms. However, these defenses are limited and avoiding a contract based on these defenses requires consumers to meet a high burden.\textsuperscript{128} As a result, there have been suggestions in the US that changes should be made to police, or control, the current tracking of consumers. Consumer rights advocates maintain that current system offers consumers too few options. Of the options available to consumers, they provide little relief. As suggested by one author, current assumption by legislators and industry “that consent in the form of a EULA clickwrap is sufficient to legitimize the practice of indefinite online surveillance” should be challenged.\textsuperscript{129} The author maintains that the privacy concerns at stake call into question the application of the contract doctrine of the “bargain of software in exchange for indefinite surveillance.”\textsuperscript{130} In the EU, regulators have limited what consumer can accept in other areas as a result of public policy concerns. In the UTCCD, blacklisted terms represent a policy decision. Although there is no prohibition on behavioral advertising, the state has made a decision that in all circumstances, certain terms will be unenforceable. A similar approach could be taken in both the EU and the US to limit blanket and essentially unlimited long-term surveillance of consumers.

From a legal point of view, it can be argued that consent has either been obtained, or it has not. Under current legal norms, consumers are bound by terms they blindly accept, even if the result is sometimes harsh. However, at the same time, courts have been unwilling to enforce agreements that fail to meet a minimal level of consent, particularly if the terms are unfair or have a harsh result for the consumer. In the next section I will present a case, regarding a behavioral advertising system, which illustrates this dynamic.

\textsuperscript{128} Winn and Webber, at 212 (2006) (\textit{Maintaining} that “U.S. online consumer contract law sets a much lower mandatory minimum level of protection [for consumers]”).

\textsuperscript{129} Barnes, at. 1610 (2006).

\textsuperscript{130} Id.
2.7 Presentation of BA terms, the case of Sears Inc.

In the US, a company omitting material terms in consumer agreement may face regulatory action for engaging in a deceptive trade practice. The FTC has the obligation to prevent “unfair or deceptive acts or practices in or affecting commerce” in the US. If the FTC suspects unfair or deceptive practices are taking place, it may issue a “cease and desist” order and stop the offending conduct. In recent years, the FTC has increased its enforcement against companies violating deceptive trade practice laws on the Internet. The following case is an example of one such enforcement.

In September of 2009, the FTC issued a complaint against Sears Holdings Management Corporation Inc. ("Sears") for alleged violations of US federal law with its use of tracking applications. In the Sears case, the FTC alleged that a software application Sears installed on its customer's computers allowed the company to track the online behavior of its consumers on and off the company’s website. The tracking by Sears included interactions with “third-party websites shopping carts, and online accounts, and headers of web-based email.” The information was then transmitted back to servers maintained by Sears for advertising and marketing purposes.

In the Sears case, the information collected was not limited to interactions on Sears’s homepage and also recorded information from online banking sessions, email and instant messages, and other consumer activities, some of which occurred during "secure" web

---

134 http://www.ftc.gov/occ/brfovrw.shtm (last visited August 11, 2010). (Providing an overview of the FTC's legal authority and mandate.)
137 Id.
138 Id.
sessions. The FTC did not determine whether the underlying Sears contract was enforceable. However, the FTC asserted that the actions of Sears were unfair or deceptive as they related to its behavioral advertising practices. For Sears, the terms disclosed in its Privacy Statement and User License Agreement (“PSULA”) failed to adequately provide the consumer with necessary information regarding the type of data it would collect. The FTC charged “that (1) the company's initial invitation email stating that the software would track online browsing was inadequate, (2) the full disclosure of the scope of tracking was buried in the 75th line of the PSULA, (3) the installation box did not disclose the scope of the tracking application, and (4) the company failed to provide any desktop tray icons or other signs to indicate the running of the application on computers.”

The FTC action was in many ways unexpected. Sears was essentially compliant with what had been considered a relatively safe and settled business practice in the US, namely, clickwrap assent. As one author noted “[i]n most respects, Sears did what nearly fifteen years of legal decisions, with only a few exceptions, have indicated make an enforceable online contract and privacy policy, namely, that the consumer is given a reasonable opportunity to review the terms of the agreement and that the user indicates assent to the agreement.” The action by the FTC may require businesses to reconsider legal aspects of contracting as it relates to the terms governing privacy. For example, in the settlement, Sears was required to take additional steps in protecting consumer privacy as a result of the earlier violation. If Sears deploys similar behavioral advertising devices in the future, it must disclose information regarding the tracking order “clearly and prominently” and on a separate screen from any “end user license agreement, privacy policy, terms of use page, or similar document.” Sears was also required to clearly provide all the information that the tracking

139 Gindin, at ¶ 1 (2009).

140 Id.


142 Fang, at 673 (2010).

143 Id. Describing the holding as a “watershed moment” in the behavioral advertising dialogue. Id. at ¶ 68.

144 Id.

application would monitor.\textsuperscript{146} The order also provides that Sears must “[o]btain express consent from the consumer to the download or installation of the tracking application.”\textsuperscript{147}

The case of Sears gives some credence to the argument that the display of terms to consumers, particularly in Browsewrap format, is insufficient.\textsuperscript{148} The tracking application Sears’s customers downloaded was extremely invasive and the information it collected was extremely broad. However, the methods used were not new, in fact, the result of this case was a surprise for many.\textsuperscript{149} What is important to learn from the Sears case is what it says about the lack of regulation governing behavioral advertising in the US. The FTC intervention was successful because Sears essentially buried the description of the application’s functions on “the 75th line down in the scroll box.”\textsuperscript{150} The disclosure of what the product did was insufficient. However, the tracking itself, absent the failed disclosure and unfair dealing, was not particularly problematic under US law. It is also important to recognize that a “fly-by-night” company did not take this action. Rather, Sears is a mainstream business and was not operating at a standard far from what is currently considered acceptable in the US.\textsuperscript{151} Based on the current regulatory landscape, had the terms disclosing the tracking application been more prominently displayed, and the functions of the tracking application fully described, the tracking system would have likely escaped regulation. Therefore, Sears tells us that although there are some protections for consumers, in particularly outrageous or extreme cases, as a whole, the lack of regulation in the US leaves businesses with wide latitude to deploy behavioral advertising technologies in online agreements.\textsuperscript{152}

\textsuperscript{146} Id.

\textsuperscript{147} Sears Order at 4.

\textsuperscript{148} Fang, at 695 (2010) (Maintaining that Sears shows the methods by which the FTC, in the future, “may enforce privacy protection under its behavioral advertising principles.”).

\textsuperscript{149} Id. at 671-72. (Maintaining that the “[c]ommission's allegations and Sears's agreement to settle surprised attorneys.”).

\textsuperscript{150} Sears Complaint at 3, ¶ 8.

\textsuperscript{151} Id.

\textsuperscript{152} Raul et al., END OF THE NOTICE PARADIGM?: FTC'S PROPOSED SEARS SETTLEMENT CASTS DOUBT ON THE SUFFICIENCY OF DISCLOSURES IN PRIVACY POLICIES AND USER
2.8 Limits to consent

The discussion of the Sears action in the previous section shows that although companies have wide latitude in applying terms in EULAs, privacy policies, and TOUs agreements, there are limits to what will be considered acceptable by regulators in the US. However, in the US, it has been argued that those remedies are far too limited. However, fears of stagnating innovation, and ultimately commerce, often hinder steps towards reform.

In the EU, when enacting laws relating to electronic commerce and online contracting, regulators have built in a much greater level of consumer protection. In the EU, “regulators have been expanding their oversight…at precisely the time that US contract law has turned away from public regulatory models.” For example, directives like the UTCCD, which provided a list of banned or “blacklisted terms” represent a policy decision in the EU. Although there is no prohibition on behavioral advertising, contract terms deemed unfair will not be enforced in the EU. A similar approach could be taken in both the EU and the US to limit blanket and essentially unlimited long-term surveillance of consumers. However, unlike the US, consumers in the EU have specific set of directives aimed at consumer protection. As a result, EU consumers have some remedies for unfair dealings, including those in behavioral advertising context. Although the Sears case suggests that some methods of disclosure will not be enforceable, the protection is reactionary, and therefore it does little to protect consumers before a problem occurs.


153 Fang, at 685 (2010).

154 Winn and Webber, at 211(2006).

155 93/13/EEC. See also 97/55/EC; 2005/29/EC for directives providing consumer protection.

156 93/13/EEC Art. 3.
3 Behavioral advertising; law, regulation, and the role of contracts and consent.

3.1 Overview and Scope

I will begin this chapter with a discussion of behavioral advertising and some of the technologies used to track online consumer behavior. The point of focus will be the legal impact of technology, rather than a discussion of technological capabilities. I will further consider the current regulation of behavioral advertising in the EU and the US. I will specifically discuss recent regulatory principles advocated by the FTC and the Working Party. In addition to discussion regarding existing regulations, I will also consider current voids in it regulation of behavioral advertising.\textsuperscript{157} I will compare the systems in place in the US and the EU, and discuss strengths and weaknesses in the current systems.

Finally I will discuss some of current causes of action and remedies available to consumers for violations of their privacy. The discussion will touch on damages consumers suffer as a result of lost or reduced privacy. In addition to case examples, I will discuss a specific case from the US showing some of the limits of data anonymization as a method of protecting consumer privacy. Next, I will compare the existing systems of regulation and provide some commentary on whether the US or the EU is dealing with the challenges presented by behavioral advertising in a more effective manner, from the perspective of the consumer. Finally, I will consider whether behavioral advertising ought to be regulated to a greater extent in either the US or the EU.

3.2 Behavioral advertising: background

The purpose of behavioral advertising is to deliver more effective advertisements to consumers.\textsuperscript{158} Behavioral advertisers use various technologies to collect information on consumer’s online behavior including cookies, adware, and deep-packet inspection. Based on


\textsuperscript{158} Hotaling, at 530 (2008).
the information collected, a consumer profile can be created. The consumer profile is designed to provide advertisers with a more accurate picture of the kinds of services or products that a user, or a group of users, might be interested in purchasing.\textsuperscript{159} The end goal of the data collection, analysis, and application is to deliver the most relevant advertisements to each user.\textsuperscript{160} It is also clear that companies across many sectors of commerce are interested in behavioral advertising as a method of increasing sales. Spending on online advertising has risen dramatically in recent years, from $6 billion in 2002 to over $16.6 billion in 2006.\textsuperscript{161} As one expert in the field succinctly stated "[t]his dream of perfect 'targeted' or 'behavioral' advertising is currently both the Next Big Thing for commerce and for funding of 'Web 2.0' businesses, but also one of the greatest potential threats we currently have to individual privacy."\textsuperscript{162}

As a result of digitalization, huge amounts of data can now be collected, stored, and searched for a relatively low cost.\textsuperscript{163} Conducting the same process via paper or analog technology would be prohibitively expensive.\textsuperscript{164} As technologies continue to improve, so does amount of data collected. At the same time advertising provider’s ability to collect and utilize data has increased, so has the number of Internet users. As of 2009, almost a quarter of the world’s population has used the Internet.\textsuperscript{165} As a result, online advertising continues to reach a greater percentage of the population.\textsuperscript{166} One company, Revenue Science Inc., maintains that it is able to track “billions of behaviors per day from more than 100 million unique users.”\textsuperscript{167} The ad

\textsuperscript{159} Edwards, Lilian. Consumer privacy law 1: Online Direct Marketing, Law and the Internet at 489 (2009).

\textsuperscript{160} Id.

\textsuperscript{161} Id.(citing George Raine, Dot-com Ads Make a Comeback, S.F. CHRON., (Apr. 10, 2005)).

\textsuperscript{162} Edwards, at 93 (2009). Capitalization in the original.

\textsuperscript{163} Id. at 448 (2009).

\textsuperscript{164} Id.


\textsuperscript{166} (availible at: http://brandedcontent.adage.com/ang/vendor.php?id=17 (last visited 30 November 2010).

\textsuperscript{167} Hotaling, at 537 (2008).
agency DoubleClick, Inc., a leading behavioral advertiser claims to have sent more than 60 billion advertisements in a single month.168

3.3 Parties involved in behavioral advertising

In this next section, I will consider the parties involved in behavioral advertising, and briefly discuss their roles in the process. Entities that produce online content, such as news websites or even bloggers are deemed “publishers.”169 Like their offline counterparts, online publishers sell space for the placement of advertisements.170 Publishers use advertising revenue to fund the creation of new products or services. The space made available by publishers, often in the form of web-banners or headers, is rented to intermediaries, often “ad agencies” or online marketers, for advertising purposes.171 Ad agencies then sell advertisements to companies and place ads in the “banners” or other space they have rented from the publishers.172 Ad agencies employ behavioral advertising technologies to sell more effective, and thus, more valuable ad space. Advertising is considered more effective if it produces a higher “click through rate” or more consumer views.173 DoubleClick, Inc., one of the largest behavioral advertising providers, contracted with over 11,000 various websites to provide them with "banner advertisements."174

3.4 Profiling approaches


169 Import, Cdt., A PRIMER ON BEHAVIORAL ADVERTISING., Center for Democracy and Technology. § 1(2008).

170 Id.


174 Id.
Profiling and digital targeting is not a new phenomenon. The first behavioral advertisements focused on the content of individual websites to deliver advertisements. For example, a news story on housing might also contain bank advertisements for loans. Initially, assumptions on readership were made based on the content of the publication. The advertiser did not explore whether the reader was interested in buying a house, selling a house, or potentially taking part in an investment opportunity. Although the first behavioral advertising methods were met with some success, this “spray and pray” method lacked the specificity of current ad systems. Although web 1.0 methods had some success, they had “inadequate user data and context upon which to judge consumer interests.”

New behavioral advertising technologies are “user-centric” rather than “site-centric.” Instead of focusing on website content, the technologies focus on the individual user. Businesses and marketing companies use available tools to collect information about online users including cookies, geographic location, click-stream data, and computer type. By combining the information they glean from these sources, behavioral advertisers can create a more relevant profile of an individual user or even a group of users. In the housing example above, the advertiser could combine the earlier search terms, along with geographic location, for clues regarding the consumer’s visit. Although the computer might have multiple users, knowing that someone at that computer conducted multiple searches for “housing styles” rather than “housing loans” is arguably valuable information for an advertiser.

The question often raised is what is the harm? Advertisers maintain that their service provides consumers with a benefit. If the consumer agreed to the tracking by contract, and

---

175 Edwards, at 489 (2009) (Stating that digital marketing commenced with the first item of SPAM email has been taking place for over 30 years).
177 Id. at 535-36.
178 Id. at 537.
179 Id.
180 Id.
181 Id.
182 Id.
the data is made anonymous, advertisers often argue that no specific harm is taking place. Regardless of the technologies employed, consumers would be delivered advertisements while accessing a publisher's service. With the second-generation technologies, at least consumers are provided with information that is potentially of interest to them. In this chapter I will consider and examine the logic behind this argument. Specifically, I will consider the limits of anonymity in advertising systems, and consider some of the resulting consequences when they fail.

The EU’s omnibus approach to data protection provides consumers in the EU with a high minimum standard of protection. Member states are given a measure of discretion in the adoption and adaptation of EU directives; however, they are unable provide protection below a minimum standard. The minimum level of protection set by the directive essentially serves as the floor or base level of consumer protection, which member states cannot drop below. Although the individual directives are designed to be comprehensive and work across multiple sectors, applicable obligations may vary from directive to directive. As a result, while certain activity may be permitted under one directive, another directive may prohibit the same activity. Therefore, ad providers must consider the mesh of regulation, and not rely exclusively on a single regulation.

### 3.5 Scope of tracking technologies considered

In this section, I will discuss some of the technologies used by behavioral advertisers. I will explain the principles of the technologies, and provide how regulations in place are applicable to them. As a preliminary matter, it is well documented that consumer information may be illegally collected by technologies such as "spyware." However, illegal technologies will not be the focus of this thesis. The discussion in this thesis is based on lawfully deployed technologies, that is, with consent of the consumer. Although I may question the presentation of terms, or the method in which the consent is obtained, I do not contend that behavioral advertising technologies should be treated in the same manner as spyware or viruses, which

---

183 Hörnle and Riefa, at 100 (2009).


185 Id.
are generally deployed without any notice to the user.\textsuperscript{186} Legislative instruments, like the ePrivacy directive, have put into place prohibitions against deployment of unlawful activity.\textsuperscript{187} As a point of departure, behavioral advertising software or adware is installed on a computer for marketing purposes, not to destroy programs, discover credit card information, or commit criminal acts.\textsuperscript{188}

Tracking of consumers on the web has rapidly evolved from systems capable of collecting information based on an individual website visited, to systems capable of tracking complete web usage by a consumer. In this section I will discuss well-established technologies such as cookies, which are used to facilitate the behavioral advertising process. Additionally, I will consider application and operation of new and future technologies, such as deep packet inspection (hereinafter “DPI”). By considering DPI, a better picture of how the current systems in the US and EU will be able to react to and regulate more advanced behavioral advertising technologies. By comparing the current and next generation behavioral advertising technologies, we can better evaluate the effectiveness of regulatory proposals made in the US and the EU.

### 3.6 Cookies

Behavioral targeting technologies utilize “cookies” which allow a website to recognize a particular user when they visit.\textsuperscript{189} Cookies are small text files, which are placed on a user’s hard drive and are recognized by a particular website.\textsuperscript{190} The amount of information retained varies and may include anything from shopping cart contents to the users Internet Protocol (IP) address or credit card number.\textsuperscript{191} Cookies have many legitimate uses in electronic commerce, and the length of time a cookie remains active on a user’s computer varies.\textsuperscript{192}

\textsuperscript{186} Barnes, at 1556-57 (2006).


\textsuperscript{188} Barnes, at 1551 (2006).

\textsuperscript{189} See www.allaboutcookies.org (last visited 24 October 2010).

\textsuperscript{190} In re Pharmatrace, 329 F.3d 9, 14 (1st Cir. 2003).

\textsuperscript{191} Siebecker, at 896 (2003).

“Session cookies” only remain active during a specific user session on a website and contain no memory past the initial visit.193 “Persistent cookies” stay on a user’s computer for multiple sessions and allow the website to recognize the user during future visits.194

Some cookies are deposited on consumers by an individual website, but are recognizable by members of an advertising network. If, for example, if a user visits iTunes,195 a cookie is deposited so that iTunes will remember the visitor in the future. This is a “second-party” cookie. If iTunes is partnered with an advertising provider like DoubleClick, an advertising cookie will also be deposited on the user's hard drive. The DoubleClick cookie is of the "third-party" variety.196 The result is that DoubleClick, a behavioral advertiser, can follow the user and track purchases on iTunes, in addition to other member sites by using the cookie technology. By storing information gathered across multiple partners’ websites, more information is collected than would be possible from any single member.197

As with many behavioral advertising applications, consumers are often unfamiliar with the technology being used. In a recent study, consumers were asked, "if you use a computer, have you ever heard of an online technology known as cookies?"198 The result was that 60% of percent of the respondents had not heard of cookies.199 Of those respondents who had heard of cookies, 25% incorrectly stated their function.200 Arguably, consumers have some control over cookies, that is, consumers may refuse to accept them if they wish. As discussed Supra, consumers may block cookies by browser settings. However, the fact that most consumers are unaware that the technologies exist, suggests that consumers may not be effective in taking proactive steps to block behavioral advertising technologies.

---

194 Id.
196 Art. 29 WP Opinion 2/2010 § 2.2.
197 Siebecker, at 899 (2003).
198 Id.
199 Id.
200 Id.
Cookies have become a well-established part of consumer web usage. Although cookie technologies may not be widely recognized by the consumers using them, regulators, particularly in the EU, have considered the role of cookies and other such technologies and their potential negative impact on consumer privacy. In the next section, I will discuss a technology that is new and is poised to strain the limits of some legislation currently in place in both the US and the EU.

### 3.7 Deep Packet Inspection (DPI) technology

DPI technology is a platform used to provide behavioral advertising to online consumers.\(^\text{201}\) The technology allows Internet Service Providers (ISPs) to collect all Internet communications by an individual user.\(^\text{202}\) Unlike other types of behavioral technology, DPI intercepts web traffic from all websites visited, and can be used to create much broader profiles.\(^\text{203}\) The information gathered by DPI is not limited by the websites an individual visits.\(^\text{204}\) Because the technology essentially intercepts communications, the user is often unaware that profiling is taking place. A browser set to reject cookies will not limit DPI tracking, because cookies are not used.

From a contractual perspective, the consumer consents to DPI monitoring via service contract with an ISP. When a consumer signs up with a provider, they agree to allow the ISP to monitor their web use.\(^\text{205}\) The ISP then contracts with a DPI firm to intercept web traffic, which is communicated between a consumer and a website.\(^\text{206}\) A critic of the technology provided the following DPI analogy: “[i]t’s like the Post Office opening all of my letters to see what I’m interested in, merely so that I can be sent a better class of junk mail.”\(^\text{207}\) On September 30, 2010 the EC brought action against the UK for “not fully implementing EU rules on the confidentiality of electronic communications such as e-mail or Internet

\(^{201}\) Person, at 436 (2010).

\(^{202}\) Id. at 438.

\(^{203}\) Id. at 442.

\(^{204}\) Edwards and Hatcher, at 532 (2009).

\(^{205}\) Id.

\(^{206}\) Id.

\(^{207}\) Edwards, at 540 (2009).
browsing.” No decisions on the use of DPI have been issued by the Working Party; however, the WP recently stated that the application of DPI technology in the behavioral advertising context “raises serious legal issues.” There have not been any court decisions regarding DPI in the US. However, it is estimated that 10% of American Internet users in the US have had their browsing monitored by DPI.

The contractual structure of used to deploy DPI is of interest. The used of DPI technology shows a continuation of the policy of using consent as a method of deploying long-term consumer surveillance for advertising purposes. However, unlike cookies or adware, DPI can potentially provide complete surveillance of consumer activity. Therefore, it is important to consider the contractual agreement, and their relation to data protection or other schemes of regulation.

3.8 FTC and Working Party principles

In the previous sections I discussed the parties involved in behavioral advertising, profiles created, and some of the technologies used. The following section will consider recent opinions or and policy statements by regulatory agencies in the US and EU. Specifically, I will consider principles that behavioral advertising companies may follow in order to be compliant with applicable law.

In 2009, the FTC provided a list of non-binding principles or guidelines that behavioral advertisers should follow to in order to avoid committing deceptive trade practices. The FTC proposal largely follows the current tradition of self-regulation in the US. In 2010, as a result of concerns regarding behavioral advertising in the EU, the Working Party adopted an opinion on the matter. The Working Party opinion provides points for behavioral advertisers


210 Person, at 443 (2010).


212 Fang, at 673 (2010) (Stating that FTC reports "do not necessarily bind industry participants, but do establish informal standards for assessing a company's privacy practices.").
to follow in order to be more compliant with EU data protection law. Neither the FTC report nor the Working Party opinion has the force of law; however, both are considered authoritative in their respective jurisdictions. Unlike the Working Party, the FTC has the authority to initiate enforcement actions against companies committing what it deems to deceptive or unfair trade practices.\(^{213}\) The main principles from the respective agencies are as follows:

<table>
<thead>
<tr>
<th>FTC(^{214})</th>
<th>Article 29 Working Party(^{215})</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Transparency and Consumer Control; (2) Reasonable Security, and Limited Data Retention, for Consumer Data; (3) Affirmative Express Consent for Material Changes to Existing Privacy Promises; (4) Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising.</td>
<td>(1) Limit in time the scope of the consent; (2) offer the possibility to revoke consent; (3) create visible tools to be displayed where the monitoring takes place; (4) Create opt-in mechanisms requiring affirmative action by the consumer.</td>
</tr>
</tbody>
</table>

The principles provided by the respective agencies will be used as a point of comparison of the approaches taken in enforcement in the US and the EU. There are clearly some common principles or points of agreement that exist between the FTC and the Working Party. When comparing the opinions, one of the points stressed by both the regulatory bodies is consumer consent. Although discussion differs, both agencies focus on the need for consumers to have a greater level of control over their grant of consent. Particularly, both agencies emphasize the need to for behavioral advertisers to obtain an “express” or “affirmative” grant of consent from the consumer before tracking online behavior. Both groups appear to have concerns with the passive nature of the consent by which behavioral advertising technologies are being implemented and tracking consumers.

\(^{213}\) 15 U.S.C. 45(a)(1) § 5. The FTC can only enforce “unfair trade practices” which should not be confused with legislation, or a specific cause of action, regarding behavioral advertising.


\(^{215}\) WP Opinion 2/2010. Points provided were highlighted in the opinion, but not provided as a self-standing or independent list.
As discussed in chapter 2, consumers often fail to read or understand terms of contracts or other agreements disclosing behavioral advertising policies. It is also very difficult for consumers to detect tracking systems after they have been installed.\footnote{Berger, at 14 (2010).} The level of sophistication of tracking technologies is difficult to comprehend, even for an expert user.\footnote{Edwards and Hatcher, at 511 (2009).} As stated by the Working Party, “[I]n most cases, individuals are simply unaware that this [tracking] is happening.”\footnote{WP Opinion 2/2010 § 6.} In addition to more complicated term disclosers, consumer protection advocates are also concerned that tracking practices are becoming more invasive.\footnote{See Electronic Privacy Information Center (“EPIC”) complaint to the FTC regarding the Google Doubleclick merger, which was ultimately approved. Available at \url{http://epic.org/privacy/ftc/google/} (last visited 12 October 12, 2010).} Many consumers do not have the tools to make coherent, informed decisions regarding behavioral targeting applications. Furthermore, the Working Party has challenged some of the behavioral targeting practices that were fairly widespread in the EU as being incompatible with EU law.\footnote{Eeck et al., at 26 (2010).}

Although some of the principles are similar, the Working Party opinion stands in stark contrast the FTC principles from the point of practical suggestions made to increase consumer privacy.\footnote{Sohn, at 786 (2010) (Arguing that the FTC Principles lack of “substantive limitations on data collection and uses, means for ensuring data quality, and mechanisms for accountability.”)} The Working Party makes specific, concrete suggestions to enhance consumer protection. Suggestions like creating “visible tools to be displayed where the monitoring takes place” would greatly increase consumer knowledge of the tracking that is occurring. Under the current system, in both the EU and the US, once an advertiser achieves consumer consent by contract or other agreement, the consumer has very few reminders that the tracking continues to take place. Because the technologies are basically invisible to all but the most technologically proficient user, most consumers are unable to determine when their activities are essentially being recorded. Additionally, creating “opt-in mechanisms requiring affirmative action by the consumer” would require more affirmative action from the consumer.
In the EU, after implementation of the ePrivacy directive, member states will allow targeting to take place only if the consumer provides adequate consent.\textsuperscript{222} As stated in the Working Party opinion, “[c]onsent must be obtained before the personal data are collected, as a necessary measure to ensure that data subjects can fully appreciate that they are consenting, and what it is that they are consenting to.”\textsuperscript{223} Therefore, pursuant to Article 5(3) of the ePrivacy directive, a cookie cannot be lawfully placed on the user’s terminal equipment, absent prior consent. As stated in section 2.5 Supra, according to the Working Party, default browser settings fail to provide adequate prior consent.\textsuperscript{224} If the consent is to be informed, information about the sending purposes of the cookie must also be provided to the user. Under the Working Party principles, even if consent is initially obtained from the consumer, the consumer will retain the power to revoke the consent at a later time. The Working Party makes it very clear that uninformed and unspecific grants of consent are inadequate.\textsuperscript{225}

On the other hand, the FTC principles use terms like “transparency and consumer control.”\textsuperscript{226} As aspirational goals, these ideas sound positive for consumers. However, the FTC fails to objectively define what this means in a meaningful context. To a consumer seeking greater protection, or a behavioral advertiser attempting to be compliant with the law, general goals or principles like “consumer control” are difficult to decipher. For example, in the Sears case discussed in chapter 2, would the company’s actions have been transparent, and thus compliant with the principles, if the disclosure of behavioral tracking terms were placed on the 15\textsuperscript{th} line of the policy rather than the 75\textsuperscript{th}?\textsuperscript{227}

In the following sections I will compare the current structures in place governing behavioral advertising practices in the EU and the US. In addition to the direct regulations, I will consider the application of consent, incorporation of contract terms, and consumer protections

\textsuperscript{222} EU member states are required to implement the directive into national law by June 2011. WP Opinion 2/2010 § 4.1.1. Emphasis added.

\textsuperscript{223} Id.

\textsuperscript{224} § 2.4 “Browser settings as a means of providing consent.”

\textsuperscript{225} WP Opinion 2/2010 § 4.1.

\textsuperscript{226} Id.

\textsuperscript{227} Fang, at 685 (2010).
that may be applicable. I will make references to the Working Party and FTC principles where they are applicable.

### 3.9 EU regulations

The EU is home to some of the most comprehensive privacy regulation in the world. EU legislation is aimed at protecting individuals from unauthorized processing of their personal data.\(^228\) EU protections include directives passed on an EU wide level, which must be adopted locally by member states.\(^229\) The scope of the EU regulations I consider will be limited to most relevant to behavioral advertising. Specifically, I will consider how EU regulations directed at protecting data work in concert with regulations protecting consumers entering into contracts. I this section I will focus primarily on the Data Protection Directive 95/46/EC (hereinafter “DPD”)\(^230\) and the ePrivacy directive.\(^231\) Although not yet applicable in all jurisdictions, the processing of personal data via Internet services will soon be governed by the ePrivacy directive.\(^232\)

In addition to protections in place under various EU directives, international conventions including the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter “ECHR”) are applicable to data processing in the EU. Pursuant to Article 8 of the ECHR, EU citizens have a fundamental right to a private life.\(^233\) As a result, under the ECHR, private individuals have a cause of action against a state, not private individual, for violations stemming from their right to a private life.

---

\(^{228}\) King, at 157 (2008).

\(^{229}\) Id.

\(^{230}\) Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

\(^{231}\) Directive 2002/58/EC.

\(^{232}\) Directive 2002/58/EC, Art. 1. The directive has been enacted in some member states and must be enacted in all states in 2011.

\(^{233}\) See Art. 8 of the ECHR (2000).
Any website visited by EU users, which installs cookies on the browser of the EU user, will be subject to European data protection and privacy laws. Therefore, American companies providing or utilizing behavioral advertising services to consumers in the EU will be subject to the regulations prescribed in the directives. The starting point for protection under DPD is to determine whether the information being provided is personal in nature. Data collected on an anonymous basis will not fall under the DPD. Although determining whether information collected is truly anonymous is not always clear, making data collected anonymous is a method used by companies to limit potential liability under the DPD.

However, simply anonymizing data may no longer be a sufficient measure of protection for behavioral advertisers. Even if ad providers escape some liability under the DPD by making data anonymous, in its opinion, the Working Party clearly took issue with the effectiveness of anonymization as a means of protecting consumers. The Working Party asserts that because behavioral advertising is based on creating very detailed user profiles, in many cases, the profiles will be deemed personal information. As provided for in Recital 24 of the ePrivacy directive “terminal equipment of users...and any information stored on such equipment are part of the private sphere of these users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms.” Because behavioral advertising employs tracking technologies, the law in the EU places additional requirements on the personal information collected.

Therefore, the information gathered by cookies for behavioral advertising purposes does not have to be personal information before it is subject to regulation. In the context of behavioral targeting, the browsing information being collected is from a private sphere, and as

---

234 Kuner, Christopher, International Journal of Law and Information Tech Vol. 0 No. 0 at. at 16 (Oxford Uni. Press 2010) (Noting that the ability to enforce this jurisdictional principle has been called into question)).

235 Id. at 2. (Discussing Article 29 Working Party Opinion 10/2006 (SWIFT)(adopted 22 November 2006)).

236 Council Directive 95/46, art. 2(a), (“information relating to an identified or identifiable natural person”).


238 WP Opinion 2/2010 § 3.2. Emphasis supplied.

239 WP Opinion 2/2010 § 3.1 (Stating that tracking consumers by use of cookies and related devices is governed by article 5(3) of directive 2002/58)).

240 Id. at § 3.2.1.
such, receives additional and independent legal protection.\textsuperscript{241} Stated differently, whether the information collected is personal in nature does not strictly control the law applicable. According to the Working Party, simply violating the protected sphere is a sufficient violation. Therefore, the act of collecting the information, regardless of the ultimate content obtained is an independent and legally significant violation of privacy according to the working party.

Pursuant to the DPD, data controllers have a much greater level of liability than data processors.\textsuperscript{242} However, this is not strictly the case pursuant to the ePrivacy directive. The requirements of article 5(3) of the ePrivacy Directive are applicable “whether the entity that places the cookie is a data controller or a data processor.”\textsuperscript{243} Therefore, the ePrivacy directive applies to individuals placing cookies, regardless of their use of the equipment.\textsuperscript{244} If the behavioral advertiser also processes personal data, they may have additional obligations as a controller pursuant to directive 95/45/EC.\textsuperscript{245} Publishers may potentially take on the role of controller, depending on the amount of visitor data provided to ad networks, and the underlying contractual agreement.\textsuperscript{246} As a result, a company providing behavioral advertising services may face liability under multiple directives for the activity. An entity engaged in behavioral advertising may also be required to comply with additional obligations under the DPD such as data retention schedule, erasure of data, and rectification of records.

In addition to obligations presented pursuant to the DPD, liability of an entity creating and using tracking applications is readily apparent under the ePrivacy directive. The recent Working Party opinion suggests that in addition to an ad company actively creating profiles based on user information, publishers may also have liability. In the general practice, publishers have been thought to have some measure of insulation from liability. However, the

\textsuperscript{241} Id.

\textsuperscript{242} Id. at 23. Stating that ad service providers and publishers may be considered joint controllers in some circumstances (example 14).


\textsuperscript{245} Id.

\textsuperscript{246} WP Opinion 2/2010 § 3.3.
Working Party has determined that even if the publisher’s actions are essentially limited to renting out banner space on a website, liability may be incurred.

Additionally, the Working Party has rejected the approach of providing an “elaborate” privacy policy, wherein the most essential information is hidden or difficult to find. This approach, which as discussed in Chapter 2 is relatively common in the US, has been abandoned in favor of providing all relevant information in a “clear and comprehensive manner.” For behavioral advertisers this may even include periodically notifying users that monitoring is taking place.

### 3.10 Opt-out v. Opt-in requirements

In the EU, the discussion on the whether behavioral advertising technologies should only be deployed on an opt-in basis has been going on for some time. In the EU, behavioral advertisers may track consumers without having them specifically choose to opt-in. However, the ePrivacy directive provides that “consent may still be made conditional on the well-informed acceptance of a cookie or similar device…”

The Working Party has stated that while opt-out policy schemes may provide consumers with increased control over their privacy, they are generally insufficient to provide for consent. The WP has noted that only in “very specific, individual cases, could implied consent be granted” by and op-out system. Perhaps users with a certain level of experience with behavioral advertising are able to provide consent in this manner. The WP does not suggest that a subjective standard should be applied. However, it follows that the sufficiency of an opt-out program is the exception rather than the rule. As a result, opt-out programs will rarely fulfill the requirement of Article 5(3) of the ePrivacy directive.

---

247 Eecke et al., at 26 (2010).
248 Id.
250 Id. at 514.
3.11 Potential causes of action against behavioral advertisers: US

In the previous section I discussed the system of regulation in the EU as it relates to behavioral advertising. In the next section I will consider some of the remedies and causes of action currently available in the US for consumers facing violations of privacy rights. I will consider the right to privacy, statutory regulations, and causes of action sounding in tort.

3.11.1 Right to privacy in the constitutional and common law

Despite references to the “right to privacy” in political discourse, the US constitution does not contain an enumerated right as such. The United States Supreme Court (US Supreme Court) has considered the right to privacy, and has concluded that a right to privacy exists; however, the right is narrow in scope and application. The US Supreme Court has recognized a cause of action for violations of privacy against government actors. The right of action is based on “several fundamental constitutional guarantees,” which exist in the Third, Fourth, and Fifth amendments to the US constitution.

As a result, citizens have recourse against government-sanctioned violations of their privacy, in limited circumstances, but not those of a private company. If one private citizen violates the rights of another, there are no specific constitutional protections in place. This does not mean that no available cause of action exists for consumers. The common law has recognized certain causes of action, generally sounding in tort, for violations of the individual right to privacy. However, the lack of constitutional protections is in contrast with the European approach, wherein a right to a private life is recognized. Although common law has

---

253 Brandeis, Warren, THE RIGHT TO PRIVACY 4 Harv. L. Rev. 193, 195 (1890)(arguing that the common law must protect the individuals right to solitude).


255 For example, and illegal home search by a government actor may violate the 4th Amendment.

256 Id.

257 Discussed Infra § 3.9.
recognized certain causes of action, generally sounding in tort, for violations of the individual right to privacy, the right is not constitutionally based.  

3.11.2 Statutorily based causes of action

The US federal government has also developed certain statutory causes of action for privacy violations. In the US, focus on privacy protections has been on individual sectors of commerce.  

This approach is in contrast with the EU, which has taken an omnibus or more global approach the protection of privacy as a right. Specifically, the financial sector has been the recipient of several such sector specific regulations. In 1978 the US Congress enacted the Right to Financial Privacy act of 1978 (hereinafter “REPA”). The Bank Secrecy Act was enacted in 1970 and provides for consumer protections related to privacy in banking transactions. The Fair Credit Reporting Act, which was enacted in 1970 limits sharing and use of certain personal information related to credit. US federal law also provides additional privacy protection for minors. Pursuant to the Child Online Privacy Protection Act (COPPA), websites must obtain parental consent before obtaining personal information regarding children. COPPA essentially provides parents with higher level of control over their children’s personal information then they have over their own privacy.

In addition to the general sector specific regulations, separate protections, including criminal penalties are available in the form of wiretapping or surveillance prohibitions. The Electronic Communications Privacy Act of 1986 (ECPA), the Wiretap Act, and the Stored Communications Privacy Act provide for causes of action against both public and private actors. Although the ECPA was enacted well before the growth modern behavioral

---

258 Id.


advertising, parties have attempted to apply it to violations of privacy rights. In the US, plaintiffs have attempted to bring lawsuits under these sections for what they believed were privacy violations online.

In addition to definitional and conceptual barriers in wiretapping statutes, plaintiffs have encountered substantial barriers in showing that the monitoring taking place was without user consent. As discussed in section 2, at some point in the contracting process, whether by clickwrap or Browsewrap agreement, consumers generally provide for consent to be monitored. In the US, if a company is able to gain consent, they will avoid enforcement under federal laws relating to electronic surveillance. For example, the Wiretap Act provides that "...an adware company that obtained consumer consent to a EULA could argue that it is immune from liability because of the consent provision of 18 U.S.C. § 2511 (2) (d)." Additionally, many of the statutory provisions protecting consumers in the US are based on activities of state actors, such as law enforcement. Therefore, the protections are ill suited for use against private companies intercepting consumer information. As a result of the broad exceptions provided, the protection granted to consumers is minimal. If a consumer consents to the surveillance, the remedies afforded under these statues will be generally unavailable.

Plaintiffs suing advertisers faced this “consent problem” in the case of In re DoubleClick consumers brought causes of actions under the ECPA against behavioral advertising companies. In the case of In re DoubleClick, DoubleClick, a behavioral advertising company, admitted to placing “cookies” on the Plaintiffs’ hard drives. Double-click further admitted that cookies, as well as other tracking technologies, monitored the plaintiff activates online for the purpose of providing advertisements. However, the DoubleClick Court held the Plaintiffs provided prior consent to the monitoring activities that took place. Even if the consent was provided via the publisher’s website, the consumers consent to a third-party


266 Id. at 1563.

267 Id. Emphasis added.

268 Id. Additionally, DoubleClick Plaintiffs also failed to show damages in excess of $5,000 as required pursuant to Computer Fraud and Abuse Act codified at 18 U.S.C. § 1030.

269 154 F. Supp. 2d at 514.
cookie was sufficient. As a result, Double Click’s surveillance fell outside of the protection of the statute.

In a case with some factual similarity, In re Pharmatrak, Inc., (hereinafter “Pharmatrak”) the plaintiffs brought claims under the ECPA.\textsuperscript{270} In Pharmatrak, the district court followed the holding in the DoubleClick and found the consent of the plaintiffs fatal to their claims to their cause of action under the ECPA.\textsuperscript{271} However, on appeal, the district courts earlier determination was reversed. The appellate court determined that notice was not provided and therefore “pharmaceutical companies [plaintiffs] did not give the requisite consent.”\textsuperscript{272} Furthermore, the appellate court found the fact that “[t]he pharmaceutical clients sought and received assurances from Pharmatrak that its NET compare service did not and could not collect personally identifiable information.”\textsuperscript{273} The Court found this assurance, that tracking was not taking place, inconsistent with consent to allow tracking.\textsuperscript{274} The Pharmatrak court also noted efforts of the defendants and found the invisible nature of the behavioral advertising technology, which was by design, provided deficient notice and invalidated any implied consent.\textsuperscript{275}

Consumer attempts at litigation under statutory acts, outside of the FTC have been met with little success. Therefore, although the ECPA may be useful in prosecuting unauthorized installations, such as the case of spyware, the act has proven difficult to apply in cases where consent is a defense.\textsuperscript{276} The Pharmatrak case shows there are some limits to implied consent, particularly in cases where a user is told behavioral tracking is not taking place. However, as a whole, the ECPA is of limited utility where consent is obtained in the behavioral advertising context.

\textsuperscript{270} 329 F.3d 9, 13 (1st Cir. 2003).
\textsuperscript{271} Id.
\textsuperscript{272} 329 F.3d at 20.
\textsuperscript{273} Id.
\textsuperscript{274} Id.
\textsuperscript{275} Id.
\textsuperscript{276} Barnes, at 1563 (2006).
3.11.3 Causes of action based in tort

In the US, the common law allows for causes of action for invasion of privacy. However, consumers also face challenges in bringing lawsuits against behavioral advertisers under this cause of action. As stated Supra, consumers are often unaware that the tracking practice is taking place. Unlike many consumer lawsuits, where a product malfunctions or an individual faces specific and obvious harm, behavioral tracking is not always easy to detect. If it is detected, consent may defeat the consumer claim, as consent is a defense which may be available. If tracking is discovered the consumer will often find it difficult to prove that any damage has occurred. Based on the multiple levels of contracts and end user agreements, it may also be difficult for the consumer to determine which party to sue.

3.12 Impact of behavioral advertising on online anonymity

Many consumers are unfamiliar with tracking and believe that they are fairly anonymous when they are on the Internet. Often, this is not the case. When utilizing behavioral targeting technologies, companies often attempt to make the user anonymous. However, the information collected is often so detailed that user can be determine individual based on the anonymous profile. If a data breach occurs, and the “anonymous” profiles are made available, the effect on consumers may not be substantially different than simply placing their name in the public sphere. For example, in 2006 American On Line (AOL) made public the search data for 657,000 of their users in an “anonymous” profile form. Based on the available search data, the New York Times newspaper was able to identify individual users.

Profile numbers assigned to AOL users contained search terms on a range of sensitive topics including queries on health and medical issues. From the information made publically available, the NYTs indentified a user based on the profile number assigned to protect her

---

278 Barnes, at 1551 (2006).
identity. Therefore, the AOL system for anonymity “was not much of a shield.”\textsuperscript{281} From this number, the New York Times was able to determine that an over-60 widow in Lilburn, Georgia, USA, conducted the searches.\textsuperscript{282} In addition to her sex, age, marital status, and geographic location, the Times was able to determine recent searches she made including: “numb fingers”, “over 60 single men” and “dog that urinates on everything.”\textsuperscript{283} In addition to searches for products, the subject conducted searches relating to various medical symptoms or conditions.\textsuperscript{284}

The above example illustrates that the collection of consumer data has the potential to impact consumer privacy.\textsuperscript{285} How information is collected, and the strength of the systems in place to protect data, are of import to consumers. If the profiles created to protect anonymity are easily linked to individuals, they do little to protect consumers. If further shows that consenting to behavioral advertising when signing up for a service, without fully understanding the agreement, may have potential consequences for the consumer.

### 3.13 Regulation: US and EU

Both the FTC and the Working Party seem to be in agreement that current grants of consent by consumers are perhaps overly broad. They also seem to agree that behavioral advertising has the potential to negatively impact consumer privacy. Based on the increase in surveillance, regulatory and advisory bodies in both jurisdictions have reacted. The practice of gaining consumer consent, via a contract or browsewrap agreement, and then almost indefinitely providing surveillance is a recognized problem in both the US and the EU. However, when you compare the systems, the similarities between the approaches to regulation diverge quickly.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{281} Id.
\item \textsuperscript{282} Id.
\item \textsuperscript{283} Id.
\item \textsuperscript{284} Id.
\item \textsuperscript{285} See e.g. Ohm, Paul, BROKEN PROMISES OF PRIVACY: RESPONDING TO THE SURPRISING FAILURE OF ANONYMIZATION, 57 UCLA L. Rev. (2010).
\end{itemize}
\end{footnotesize}
The EU system provides for a much higher level of consumer protection on multiple levels. In addition to contractual based protections, the ePrivacy directive and the DPD provide consumers with greater levels of protection over their information even after they agree to having it collected.\textsuperscript{286} The Working Party has also taken a very consumer orientated approach in its interpretations of regulations. In the US, regulations are not as protective of consumers. Consumers have very few protections when agreements are being formed. For a consumer to escape enforcement of a term, they must generally show that the terms of the agreement are unconscionable and in some way “shock the conscious,” are “surprise or unexpected,” or should be void or for public policy reasons. In the US, the post-contractual US rights also have a very high standard of proof, and thus, are difficult to utilize for consumers. As seen in the AOL searcher example above, the failure to provide regulation and allowing profiling to take place, has an impact on consumer privacy.

\textsuperscript{286} See e.g. 93/13/EEC; 97/55/EC; 2005/29/EC.
4 Conclusion

In this thesis, I considered the role of contracts and other agreements used to legitimize behavioral advertising technologies. I maintain that online contracts, privacy policies, and TOUs agreements generally provide consumers with insufficient information to consent to behavioral advertising. The grant of authority provided in the agreements is often much broader than is understood by the consumer. Additionally, tracking technologies are more invasive than consumers are generally aware of and also track the consumer for long periods of time. The methods used to gain consumer assent, particularly browsewrap agreements, do not provide consumers with sufficient notice of the terms to which they are agreeing.

Comparing regulatory systems, the EU provides much a higher level of consumer protection when entering into agreements. By barring certain terms and allowing for post-contractual reformation of contracts, the EU provides consumers with a greater level of protection when entering into an agreement. The gap in protection is particularly prominent in the US. The common law, and modified statutory law where applicable, provide consumers with very little protection either in accepting the agreements or post-contractual rights to reform agreements. The reactionary system of consumer protection also fails to provide protection until after a problem has occurred. Unlike the EU, the US system provides consumers with too few tools when entering into online agreements.

When considering the systems governing behavioral advertising, the EU has a much more complete system to protect consumers. A major weakness with the US system, in addition to the absence of direct regulation, is overly broad consent exceptions in the few statutory protections that do exist. Stated differently, the consent exceptions swallow up any protection the statutory regulations might have provided. The EU system of providing consumers with protection at the contracting stage on the front end, and requiring higher levels of consumer protection once data has been collected, provides consumers with a much higher level of overall protection. I have considered the policies put forth by the Working Party and compared them to those of the FTC. It is my opinion that the EU system is moving further into the “fine-tuning” phase of behavioral advertising regulation while the US is still attempting to establish the ground floor. The current trends in spending on online ads suggest that behavioral advertising will be with us for some time to come. The EU system is in a better position to adapt to future challenges which will be posed by technologies like DPI.
References

EC Directives


Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (O.J. No. L 281, 23.11.1995, 31).


Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (O.J. No. L 281, 23.11.1995, 31).


2005 UN Convention on the Use of Electronic Communications in International Contracts.
European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8 (ECHR).


**US Statutes**


**US Model Acts**


**List of Judgments/Decisions:**


CompuServe, Inc. v. Patterson, 89 F.3d 1257, 1260-61 (6th Cir. 1996).


In re Pharmatrack, 329 F.3d 9 (1st Cir. 2003).
ProCD v. Zeidenberg, 86 F.3d 1447 (7th Cir.1996).
Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002).

FTC Opinions and Guides:

Electronic Privacy Information Center (“EPIC”) complaint to the FTC regarding the Google DoubleClick merger, which was ultimately approved. Available at http://epic.org/privacy/ftc/google/ (last visited 12 October 12, 2010).


Art 29 Working Party:

Art. 29 WP Opinion 2/2010 § 2.2 (adopted on 22 June 2010)

Art. 29 WP 29 Opinion 1/2008 on data protection issues related to search engines (adopted on April 4, 2008)

Art. 29 WP 29 Opinion 1/2010 on the concepts of “controller” and “processor,” (adopted on Feb 16, 2010).

Literature


Secondary Literature


Eecke et al., RECENT EVENTS IN EU INTERNET LAW—EUROPE, 14 No. 3 Internet L. 25 (2010).


Import, Cdt., A PRIMER ON BEHAVIORAL ADVERTISING., Center for Democracy and Technology, § 1(2008).


Nuth, Maryke ELECTRONIC CONTRACTING IN EUROPE; BENCHMARKING OF NATIONAL CONTRACT RULES OF UNITED KINGDOM, GERMANY, ITALY AND NORWAY IN LIGHT OF THE ELECTRONIC COMMERCE DIRECTIVE, Senter for rettsinfomatikk. (2008).


Oakley, Robert L. FAIRNESS IN ELECTRONIC CONTRACTING: MINIMUM STANDARDS FOR NON-NEGOTIATED CONTRACTS, 42 Houston L. Rev. 1041 (2005).


Pop, Valentina, EU takes Britain to court over online data protection (October 6, 2010). http://euobserver.com/22/30935

Radin, Margaret Jane. HUMANS, COMPUTERS, AND BINDING COMMITMENT, 75 Ind. L.J. 1126 (1999).


Sohn, David, REFOCUSING THE FTC’s ROLE IN PRIVACY PROTECTION, COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY IN REGARDS TO THE FTC CONSUMER PRIVACY ROUNDTABLE, 994 PLI (2010).

Steiner, Peter; published by The New Yorker on July 5, 1993 (cartoon caption).


Warner, Richard, TURNED ON ITS HEAD?: NORMS, FREEDOM, AND ACCEPTABLE TERMS IN INTERNET CONTRACTING., 15 No.5 Internet L. 18 (2010).

