‘Wrap Contracts and Privacy

Nancy S. Kim
Associate Professor, California Western School of Law
225 Cedar Street, San Diego, CA 92101
nsk@cwsl.edu

Abstract

Websites often use ‘wrap contracts — clickwrap and browsewrap agreements — which include provisions that permit websites to track and exploit customer information. In this paper, I propose that the law conceptualize a website user’s act of inputting or uploading information as constituting a limited license to the website to use the information for very expressly defined purposes. Websites that desire to use the information for purposes other than these narrowly defined ones should craft online agreements so that the user/licensor must physically indicate agreement with the nature and scope of the license by clicking once for every line containing a right or use permitted by the licensee. Incorporating a technological burden or hassle negatively affects the user’s experiences and may give less intrusive companies a competitive advantage over more intrusive ones.

Introduction

Websites often use ‘wrap contracts — clickwrap and browsewrap agreements — to establish legal relations with site visitors. A visitor to a website typically has no ability to negotiate or modify such agreements. Courts have generally recognized the validity of these online contracting forms provided that the user had notice of their existence on the site and the terms were not unconscionable.

Online agreements typically include provisions that permit the websites to track and use visitor data. Given the recent publicity in the news media about website tracking of customer information, some users may be aware of the general existence of such practices even if they themselves have not bothered to read the ‘wrap contracts of the sites they regularly use. But even those users that have some knowledge of website customer privacy practices may not have an accurate perception of the nature or extent of such practices. Websites may respond to customer ignorance or inaction by inserting increasingly more aggressive and intrusive terms in ‘wrap contracts unless and until consumers and consumer advocacy groups demand protective regulatory action. Regulatory action may come with its own drawbacks, including ineffective disclosure requirements or a ban on types of tracking that customers may want. In this paper, I argue that websites must adopt corrective measures to forestall regulation of how websites may communicate privacy policies to users. These corrective measures involve the implementation of technological measures that mimic the safeguards that were traditionally incorporated into contract doctrine prior to the advent of mass consumer agreements. I will first examine the problem of online agreements that exploit their commercial power by overreaching and intrusive privacy terms. Next I will discuss my proposed solution.

With Bargaining Power, Came Greed

The model upon which contract law is based is that of two parties negotiating terms that are to his or her advantage. Contract law doctrines were shaped in accordance with this model and persisted even as society changed so that the model no longer reflected every – or even most – commercial transactions. Thus, as mass market sales became possible with industrialization, so did mass consumer form contracts. Given the impracticability of negotiating, modifying or even discussing contractual terms with each of its consumers, companies found it much more convenient and efficient to create standard terms for standard business transactions. The courts accommodated changing market realities by enforcing these “contracts of adhesion”, i.e. non-negotiated form agreements drafted by one party and signed by the other.

Similarly, ‘wrap agreements evolved from a business reality confronted by software companies. At the beginning of the era of personal computers, some software producers were uncertain whether copyright law protected software. Because digital information could be easily copied and distributed, many software producers insisted upon licensing their software rather than “selling” it, thus avoiding the first sale doctrine.[1] The license was granted by using a mass market contract but one that didn’t incur the transactional hassle of having the customer sign anything. Thus was the “shrinkwrap” license born, and with it the whittling away of traditional contract law requirements of manifestation of assent. Courts held that the mere ripping away of plastic constituted contractual assent. "Clickwraps" required even less physical actions – a mere click of a mouse on a computer. "Browsewraps" or terms of use require still less physical manifestations of

[1] Step-Saver Data Systems, Inc. v. Wyse Technology, 939 F.2d 91, 96 n.7 (3rd Cir. 1991)(noting that form licenses were first developed for software largely to “avoid the federal copyright law first sale doctrine.”)

assent, necessitating merely that there be constructive awareness on the part of a user.

This is where greed comes in. While the willingness of the courts to accommodate market realities is admirable, the willingness of websites to capitalize on the deterioration of one foundational contract doctrine — contractual assent — to pervert the meaning of another — consideration — is truly alarming. While a website user may trade or "bargain" personal information for some purposes, it may not know that it has also unwittingly permitted much more intrusive uses. In some cases, the user may have declined to use the website if it had known about those other uses.[2] The user desires to enter into one type of bargained for exchange but has, in fact, entered into another, far more intrusive, one due to the attenuated nature of assent represented by online agreements.

For example, on the msn.com website, a user is notified of the existence of Microsoft's privacy policy only by scrolling down to the very bottom of the page. The link merely states "MSN Privacy." The user must click on those words in order to reach a second page which provides certain "highlights" of Microsoft's privacy policy. These highlights include general statements, such as "When you register for certain Microsoft services, we will ask you to provide personal information. The information we collect may be combined with information obtained from other Microsoft services and other companies." Revelations about their user tracking policy is given a consumer-friendly spin, as though such a policy were intended primarily to benefit the consumer, "We use cookies and other technologies to keep track of your interactions with our sites and services to offer a personalized experience." The highlights page provides a link to another page for the full privacy statement. The privacy statement reveals that these "other technologies" include "website analytics tools" used to "retrieve information from your browser, including the site you came from, the search engine(s) and the keywords you used to find our site, the pages you view within our site, your browser add-ons, and your browser's width and height." They also include "cookies and web beacons… to collect information about the pages you view, the links you click and other actions you take on our sites and services." Microsoft also collects "certain standard information that your browser sends to every website you visit, such as your IP address, browser type and language, access times and referring Web site addresses" and delivers advertisement and provides "Web site analytics tools on non-Microsoft sites and services, and we may collect information about page views on these third party sites as well." To opt-out of receiving personalized advertisements, the user can click on another link. Alas, the user soon discovers that opting out does not mean that customer tracking will cease, as "even if you choose not to receive personalized advertising, Microsoft will continue to collect the same information as you browse the web and use our online services. However, this information and any information collected from you in the past won't be used for displaying personalized ads."

The highlights page indicates that a user may contact Microsoft to opt-out of receiving emails or personalized advertisements. The highlights page, however, does not permit the user to opt-out from this page. In order to opt-out of receiving emails, the user must click on another hyperlink which transports the user to still another page. This page breaks down email communications into several different categories, depending on both the type of communication and the type of service. In other words, the user cannot opt-out of all Microsoft email communications at one time – he or she must address each type of communication for each type of service separately. The user's quest to opt-out of emails, however, doesn't end there. If the user decides to opt-out of marketing communications from Microsoft.com, for example, the user must click on that category and is sent to the Microsoft.com Profile Center. Here, even a persistent user may be mystified for there is no indication on this page that the user may opt-out of marketing communications. Instead, the front page links state "Update your personal information," "Update my contact preferences," "Update my technology interests," etc. From there, the user must again select a category. At that point, the user is then sent to a page where he or she is required to sign in to his or her Microsoft account in order to then opt-out of receiving marketing communications.

Other websites are not as demanding as Microsoft, but many of them do bury their privacy policies and terms of use at the bottom of web pages, in small print and past the page break – necessitating scrolling on most computers and multiple clicks to opt-out or register disagreement.

Implementing Technological Measures that Manifest Actual Assent

As the previous section illustrates, some companies have implemented 'wrap contracts to do much more than combat unfair or infringing conduct — they have used them to implement unfair business practices that can deceive, annoy and manipulate consumers into relinquishing personal information.

The judiciary's recognition of 'wrap contracts reflected an admirable policy of encouraging innovation and accommodating the needs of the fledgling software industry. The overreaching by some websites should not delegitimize the *form* of 'wrap agreements; rather it should indicate that the form needs some adjustments. In other words, to recognize that online agreements are not *per se* invalid should mean neither that all online agreements are valid nor that every provision in an online agreement is enforceable. Instead, I propose that websites should im-

[2] A recent survey indicates that two-thirds of respondents were opposed to online targeted advertisements and that it matters to them how their movements are being tracked. *See* Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley and Michael Hennessy, *Contrary to what marketers say, Americans Reject Tailored Advertising And Three Activities That Enable It* (2009).

plement technological measures that require users to manifest actual assent to certain provisions. The user would not be required to manifest assent to the permission to use the website (typically, under the "license grant" provision") or to the description of provided services. Both provisions merely explain what the website is offering the user. These types of provisions do not purport to take away any rights from or impose any obligations upon the user. In other words, provisions that explain what rights the website is giving up or what services it is obligating itself to provide do not require actual assent. The user has no right or obligation to force or change the nature of the website's business by, for example, demanding different services or products. Accordingly, the user's assent can be presumed.

Other provisions, however, should require a manifestation of actual assent by the user. These provisions would be those that seek to use information provided by the user, such as personal identifying information, or purport to wrest away from the user certain rights that it would otherwise have. In essence, what website privacy policies and 'wrap agreements do is give websites a license to use customer information. Contract law should recognize that when a user inputs or uploads content, the user is granting the website an implied limited license to use that content solely for the stated purpose – i.e. to process a credit card transaction or to register as a site member. If the website wants to use the content for other purposes, such as selling the information to marketers, it must obtain a broader license. The practical problem is that because the licensees, and not the licensors, draft the license, they tend to draft these licenses in very broad terms which favor the licensee.

The law must recognize that the impracticability of requiring individually negotiated agreements in mass consumer transactions cuts both ways. While there may be legitimate business reasons for utilizing 'wrap agreements, the user should not be the only party to bear the burden of a contracting form that primarily benefits the website. Because the user/licensor is the party granting the website a license to use its personal information, the online agreement should be structured to require the user to actively assent to indicate the nature and scope of that license. The interaction between the user and the website would stop until the user has manifested assent to the type of information that the website would like to exploit and the ways in which the website would like to exploit it. The more uses that the website wants for the information, the more it has to "bargain" for them, by requiring a corresponding click. I propose that a click be required after each line that contains a type of information or a type of use, i.e. the "scope" of the license granted by the user to the website. Consequently, websites could no longer hide their privacy policies and terms of use in interior pages that require multiple clicks to access.

The business risk for the website, of course, is that the more clicks a user faces, the greater the likelihood that the user will abandon the interaction; the fewer clicks, the greater the user appreciation. But that is precisely why these additional clicks should be required – ease of use would then correlate with relinquishment of rights or information. Companies that greedily seek more uses for customer data would be at a competitive disadvantage from those companies who use customer data for more narrowly defined purposes. The result is an interaction that resembles an actual "bargained for exchange", where the website must balance the uses with the risk of user abandonment and the user has greater ability to "craft" a license that reflects his or her intent in entering into the contract.