Just-In-Time Click-Through Agreements: Interface Widgets for Confirming Informed, Unambiguous Consent

Patrick, Andrew

Publisher's version / Version de l'éditeur:

Journal of Internet Law, 9, 3, 2005

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC · CNRC

Just-In-Time Click-Through Agreements: Interface Widgets for Confirming Informed, Unambiguous Consent *

Patrick, A.
2005

* published in Journal of Internet Law. Volume 9, Number 3. pp. 17-19. 2005. NRC 48256.

Canada

Author's Preprint – Citation: Patrick, A.S. (2005). Just-in-time click-through agreements: Interface widgets for confirming informed, unambiguous consent. *Journal of Internet Law, 9*(3), 17-19. (NRC 48456)

Just-In-Time Click-Through Agreements: Interface Widgets for Confirming Informed, Unambiguous Consent

by Andrew S. Patrick [*1]

The most common method for supporting consent in computer applications is a "user agreement." When you have installed new software on your computer, or signed up for an Internet service, you have undoubtedly seen an interface screen that presents a User Agreement or Terms of Service. In order to continue, you have had to click on an "I Agree" button or an equivalent label. These interface screens are commonly called "click-through agreements" because the users must click through the screen to get to the software or service being offered.[2] (An alternative label is "click-wrap agreement," in parallel to more traditional "shrink-wrap" agreements attached to software packaging.) These agreement screens are an attempt to provide the electronic equivalent of a signed user agreement or service contract.[3] By clicking on the "Agree" button, the user is confirming their understanding of the agreement and indicating consent to any terms or conditions specified in the accompanying text.

Click-Through Agreements are Binding

The legal effectiveness of these click-through screens in forming the basis of a legal agreement or contract has been established, but with some qualifications. The Cyberspace Law Committee of the American Bar Association has reviewed the case law and developed a set of guidelines for creating click-through agreements.[4] These guidelines can be been summarized into six principles that should be considered by system developers:[5]

[*] Andrew S. Patrick is a Senior Scientist in the Institute for Information Technology at the National Research Council of Canada in Ottawa.

1. Opportunity to review terms: users must view the terms of the agreement before consenting to the agreement. A case involving Netscape[6] suggests that it is important that there is no other method to obtain the product or service other than by clicking through the agreement.

2. Display of terms: the terms have to be displayed in a "reasonably conspicuous" manner. A case involving Ticketmaster[7] suggests that simply linking to the terms at the end of a long home page was not enough.

3. Assent to terms: the language used to accept the agreement must clearly indicate that a contract is being formed.

4. Opportunity to correct errors: there should be a method for users to correct errors, such as seeking a final confirmation before proceeding, or allowing the user to back out of an agreement.

5. Ability to reject terms: the option to reject the terms of the agreement should be clear and unambiguous, and the consequences of the rejection should be stated (e.g., "if you do not agree, you will not be able to use this software").

6. Ability to print the terms: the interface should allow the user to print the terms for later reading. Printing the terms will also allow the users to save at copy of the terms at the time of the agreement, which can be important for online services where the terms may change.

Other considerations when creating click-through agreements are to redisplay the terms and conditions at product startup (reminding), and to support the ability to review the terms at any time (e.g., in the "help" or "about" menus). In addition, developers should adapt the terms and conditions to local languages and requirements. If these principles and considerations are heeded, case law suggests that there is an increased chance that click-through agreements will be enforced, at least in US courts.

In fact, some recent decisions have shown that the courts are willing to enforce click-through agreements rather broadly. In a controversial case still under appeal, the U.S. District Court for the Eastern District of Missouri ruled in *Davidson & Associates, Inc. v. Internet Gateway*[8] that a special anti-reverse-engineering clause was effective. In this case Internet Gateway created a

game emulator ("bnetd") that is compatible with Davidson's Battle.net system. Because Davidson had included a section banning reverse engineering in their user agreement, the court ruled that the defendants, by accepting the agreement, had waived their fair use rights that were normally protected by copyright laws.[9]

Making Click-Through Agreements Usable

The text of many click-through agreements tends to be long and complex, often to ensure that all the points raised above are addressed. The result is that users have difficulty reading and understanding the documents, and many users click the "Agree" button without reading the terms at all. Not only are users not motivated to read the agreements, but people also have limited cognitive abilities – we have limited attention spans, a restricted ability to process large quantities of detailed information at one time, and limited memories. The result is that most user agreements are rarely read by users, with one study reporting a 0.5% reading rate.[10]

Whether users actually read the user agreements before clicking an "Agree" button is not important. For example, in *Cairo, Inc., v. CrossMedia Services Inc.*[11], the U.S. District Court for the Northern District of California ruled that, although Cairo claimed to not have read or agreed to CrossMedia's click-through agreement, because Cairo made "repeated and automated" access to CrossMedia's website, there was an imputed assent to the terms of service. Thus, the court found that CrossMedia's terms of service were enforceable even if the user did not read the agreement.

In a contrary finding, however, the U.S. District Court for the District of Minnesota dismissed a class-action lawsuit against Northwest Airlines[12] in part because the plaintiffs did not actually read the privacy policy on Northwest's web site, so their expectation of privacy was low. The plaintiffs had sued Northwest because travel records containing personal information had been given to NASA without the permission of the travelers, an act that was in apparent conflict with Northwest's own privacy policy. The court dismissed the action for a number of reasons, but the portion of the decision related to not reading the privacy policy seems to be counter to other decisions and controversial. If this precedent is adopted by other courts, the implication is that if users are required to read privacy policies before they are enforced, then it follows that companies may not be able to enforce their user agreements unless they can demonstrate that users actually

read them, although it is difficult to draw direct comparisons between decisions related to privacy rules and those related to contracts.[13]

In the area of privacy, ensuring that users fully understand and unambiguously agree to agreements and contracts is also important for complying with privacy legislation and guidelines. Consider the definition of consent provided in the EU Directive 95/46/EC on privacy protection:[14]

> 'the data subject's [user's] consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. (Article 2-h)

It is clear that a large, cumbersome, complicated User Agreement presented to the user only when they begin to use a product or service fails to live up to the requirements for "specific" and "informed" consent, and yet these types of user agreements are the majority. These issues are of particular concern in relation to explicit consent. For example, the EU Directive states that when sensitive data (e.g., race, ethnic origin, religious beliefs) are processed, the user must give "explicit consent" (Article 8-2-a) to the processing of the sensitive data. Again, a single, large, click-through User Agreement does not meet the spirit of the Directive.

After reviewing the user-based requirements for meeting the objectives of the Directive, I have proposed a new concept of "Just-In-Time Click-Through Agreements" (JITCTAs).[15] These are interface windows that appear in a display at an appropriate time to seek agreement with a key term or condition. The main feature of a JITCTA is not to provide a large, complete list of service terms but instead to determine the understanding or consent on an as-needed basis. These small agreements are easier for the user to read and process, and facilitate a better understanding of the decision being made in context. Also, the JITCTAs can be customized for the user depending on the features that they actually use, and the user will be able to specify what terms they agree with, and those they do not, and then only have access to the corresponding portions of the program or service. The responses made by the user during the JITCTAs can also be recorded so there is a clear, unambiguous record of the specific agreements made with the user. In order to implement JITCTAs, the software recognizes when users are about to use a service or feature that requires that they understand and agree to some term or condition.

A sample screen capture of a JITCTA is shown in Figure 1. In this example a user has selected the Trade Union Membership information field in an interface screen. Since this would be considered sensitive information in the EU Privacy Directive, a JITCTA has appeared to obtain explicit, timely, unambiguous consent to the processing of this data.

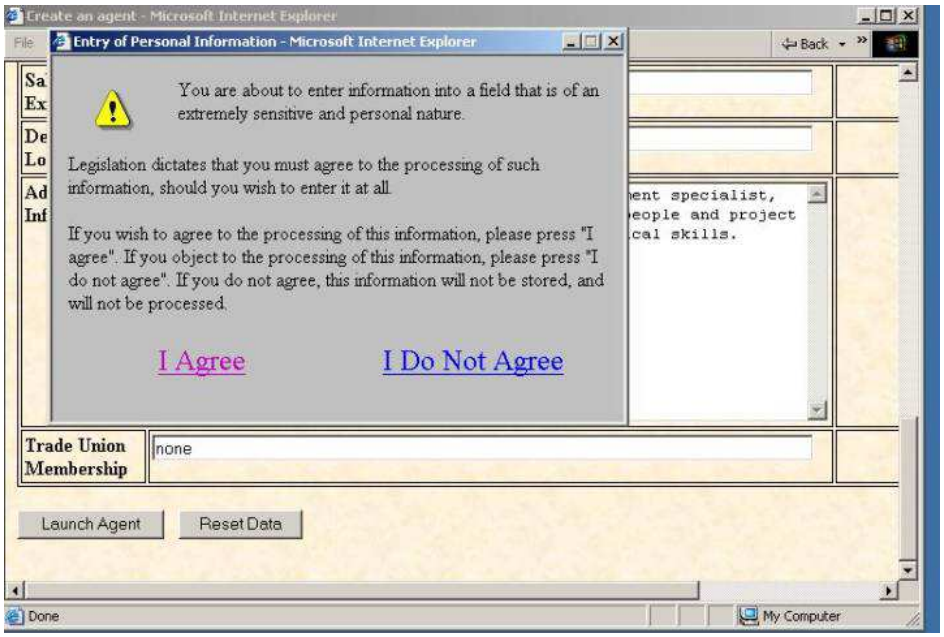

Figure 1: An example of a Just-In-Time Click-Through Agreement (JITCTA)

An empirical evaluation of the effectiveness of this JITCA technique was conducted using a prototype job searching tool.[16] Reaction to the pop-up window was mixed, with some users appreciating the information about the sensitive content being requested, while others found the interface to be annoying or they ignored the message completely. A few users justified ignoring the window with the belief that "all pop-up windows are advertisements." An alternative interface that presented the just-in-time message within the browser window, clearly associated with the interface component requesting the sensitive information, might not have been ignored so easily, although it could be found to be even more annoying.

This integration of the agreement terms and the interface components requesting personal information was examined in a study by Alfred Kobsa and Maximilian Teltzrow.[17] These researchers looked at the scenario of a book seller requesting personal data to be used when making purchase recommendations. The study examined the effect of adding additional contextual information about the benefits to the user if they provide the data (e.g., we will be able

to search for books by your favorite authors) and what will happen with their data (e.g., your list of favorite authors will be stored under a pseudonym and will not be shared with others). The experimental results showed that people were more willing to provide personal information when the agreement information was provided in context than when it was omitted, and they were slightly more likely to complete a book purchase. The study also found that none of the users chose to read a traditional, optional, long user agreement.

The concept of just-in-time user agreements is also being extended in the Privacy and Identity Management for Europe (PRIME) project, whose goal is to create systems for controlling information about users that are usable, acceptable, and in compliance with laws and regulations. Interface designers in this project have developed a graphical form of JITCTA where users express their consent to the processing of data by moving a representation of their data (an icon) on a graphical display.[18] For example, agreeing to provide personal information to a bank might be indicating by dragging a folder symbol representing personal data to a building symbol representing the bank. The PRIME developers have labeled this concept "drag-and-drop agreements" (DADAs). It is not clear whether DADAs will be treated by the courts in the same manner as click-through agreements, although it is likely since users are taking an explicit action to indicate their consent. Current research in the PRIME project is testing users' acceptance of this new agreement method.

In each of these examples, just-in-time agreements are used when a service is requesting personal information. These situations are ideal for JITCTAs because the agreement components can be separated so that individual consent verification can be obtained at the appropriate time. Moreover, it is likely that the service can proceed if the user agrees to some, but not all, of the terms and conditions. The JITCTA concept is less appropriate for software installations from CDs which tend to have an all-or-none agreement that the user must accept in its entirety. However, presenting each of the key sections of the agreement in turn would likely assist the users in understanding all the conditions that they are agreeing to. An open question is whether typical users are motivated (or should be motivated) to fully understand the agreements that are involved when installing software.

In summary, well formulated click-through agreements are usually legally binding, but there are issues with their content and how they are presented. Just-In-Time Click-Through Agreements are being explored for interfaces seeking consent to the processing of private information, and

they may also be useful for user agreements and service contracts. JITCTAs can improve the current practice by making the agreements easier to read and understand, thus supporting more appropriate decision-making and control.

NOTES

---

1 Thanks to John D. Gregory for helpful comments on this article. All errors and omissions, however, should be attributed to the author.

[2] C.L. Kunz, J. Debrow, M. Del Duca, and H. Thayer, "Click-Through Agreements: Strategies for Avoiding Disputes on Validity of Assent," *Business Lawyer*, 57, 401 (2001).

[3] F.M. Buono & J.A. Friedman, "Maximizing the Enforceability of Click-Wrap Agreements," *Journal of Technology Law & Policy*, 4(3) (1999)

[4] Kunz *et al.*, *supra* n. 2.

[5] T.D. Halket & D.B. Cosgrove, "Is Your Online Agreement in Jeopardy?" *CIO Magazine* (2002), available at http://www.cio.com/legal/edit/010402_agree.html; see also D.M. Crawford & S.L. Tupper, "Making Electronic Signatures Stick," *Michigan Bar Journal*, March, 24-28 (2003).

[6] Specht v. Netscape, No. 01-7860 (L) (2d Cir., October 1, 2002); see also the discussion in C. Martin & D. Oshinsky, "Legal Developments in Click-Wrap Licenses Raise Concern for Software Developers and Web Site Operators," *Software Council of Southern California Newsletter*, November (2002), available at http://www.scsc.org/scribeonline/legalclickwrap.html

[7] Ticketmaster Corp. v. Tickets.com, Inc., 2000 U.S. Dist. Lexis 4553 (C.D. Ca., March 27, 2000); discussed in Kunz *et al.*, *supra* n.1.

[8] Davidson & Associates, Inc. v. Internet Gateway (ED Mo, 9/30/04); sometimes referred to as Blizzard v. BNETD

[9] for a discussion, see http://www.eff.org/IP/Emulation/Blizzard_v_bnetd/

[10] R. Kohavi, "Mining E-Commerce Data: The Good, the Bad, and the Ugly," *Proceedings of the Seventh ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Francisco, 8-13, (2001).

[11] Cairo, Inc. v. Crossmedia Services, Inc., 2005 WL 756610 (N.D. Cal. Apr. 1, 2005). It should be noted that this is an "unpublished" decision so its role as a precedent is questionable.

[12] In re Northwest Airlines Privacy Litigation, U.S.MN, 6 June 2004

[13] A.C. Raul, E.R. McNicholas & J.M. Dwyer, "Federal Court Finds No Breach of Internet Privacy Policy Absent Allegation That Plaintiffs Had Actually Read the Policy," (2004), available at http://www.sidley.com/cyberlaw/features/netprivacypolicy.asp

[14] "European Union Directive 95/46/EC of the European Parliament and of the Council 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," available at http://www.cdt.org/privacy/eudirective/EU_Directive_.html

[15] A.S. Patrick & S. Kenny, "From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interfaces," In R. Dingledine (Ed.), *Proceedings of Privacy Enhancing Technologies Workshop (PET2003)*, Dresden, Germany, 26-28 March, LNCS 2760, 107-124, (2003).

[16] A.S. Patrick, S. Kenny, C. Holmes & M. van Breukelen, "Human Computer Interaction," In G.W. van Blarkom, J.J. Borking & J.G.E. Olk (Eds.). *Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents*. College Bescherming Persoonsgegevens, Den Haag, The Netherlands, (2003), available at http://www.andrewpatrick.ca/pisa/handbook/handbook.html.

[17] A. Kobsa & M. Teltzrow, "Contextualized Communication of Privacy Practices and Personalization Benefits: Impacts on Users' Data Sharing and Purchase Behavior," In D. Martin and A. Serjantov, (eds): *Privacy Enhancing Technologies: Fourth International Workshop, PET 2004*, Toronto, Canada. Springer LNCS 3424, 329-343, (2004), available at http://www.ics.uci.edu/~kobsa/papers/2004-PET-kobsa.pdf

[18] Prime Project, "Evaluation of Early Prototypes," Privacy and Identity Management for Europe (PRIME) Project Deliverable D06.1.b, (2004), available at http://www.prime-project.eu.org/public/prime_products/deliverables/eval/pub_del_D06.1.b_ec_wp06.1_V4_final.pdf