



January 9, 2015

CLIENT ALERT

Clicking Away Your Right to Privacy: Agreeing To Certain Terms in an ISP Terms of Service May Waive Your Right to Privacy

Before using any standard third party internet service provider (i.e., Gmail, AOL, Yahoo) (collectively, an “ISP”), a user first must agree to the ISP’s terms of service agreement by clicking a seemingly innocuous “I Agree” button. Most users fail to read the terms and simply click the “I Agree” button without a second thought.¹ That simple act, in certain circumstances, may waive the individual’s right to privacy.

The Origin of the Right to Privacy

Although the U.S. Constitution does not explicitly provide individuals with a right to privacy, the U.S. Supreme Court has found an implicit right to privacy couched in the Fourth Amendment to the Constitution.² The Fourth Amendment protects the right of individuals to be secure against “unreasonable searches and seizures.” In extending that right to include a right to privacy, U.S. Courts have held that if (i) an individual expects certain information will remain private and (ii) society is prepared to recognize that expectation as reasonable, then the Fourth Amendment regulates governmental investigation of that information, thereby curtailing what otherwise would be an unreasonable search and seizure.³

Applicability of the Third Party Doctrine

The general rule regarding an individual’s right to privacy with respect to information he or she voluntarily discloses is set forth in the “third party doctrine,” which holds that if a person

¹ See Jason Turrow, et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3.3 I/S: A Journal of Law and Policy for the Information Society 723, 740 (2008), available at

http://www.ntia.doc.gov/files/ntia/comments/100402174-0175-01/attachments/FTC_and_privacy.pdf (Reporting a study’s findings that only 1.4% of participants indicated they read end-user license agreements often and thoroughly).

² *Griswold v. Connecticut*, 381 U.S. 479, 85 S. Ct. 1678 (1965).

³ *Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507 (1967).

voluntarily discloses information to a third party, that person has no reasonable expectation to privacy concerning that disclosed information.⁴

Notwithstanding the third party doctrine, the U.S. Supreme Court has held that merely disclosing information to a third party does not automatically permit intrusion by law enforcement. The Supreme Court reasoned that in the current digital age, in the course of carrying out mundane tasks, individuals routinely reveal much personal information to third parties, making it necessary to consider that the individual may have a reasonable expectation to privacy regarding the information voluntarily disclosed to third parties through technology, such as an ISP.⁵

Despite acknowledging the challenge that technology brings to privacy issues, the recent *DiTomasso* case cuts deeply into Fourth Amendment protections concerning email communications.⁶ *DiTomasso* questioned AOL's right to scour an individual's emails, and if it suspected the emails to be criminal or to involve criminal activity, to turn them over to law enforcement. Although the Court in *DiTomasso* recognized an individual's general right to privacy in email communications, it went on to hold that an individual does not have a right to privacy of its emails with respect to an ISP that maintains terms of service that expressly (i) disallow criminal activity and (ii) state that the ISP monitors emails for such activity and reserves its right to take any action it deems warranted, including sharing information and cooperating with law enforcement. Moreover, the Court held that by agreeing to an ISP's terms of service (effectively, by clicking "I Agree" to an ISP's terms of service agreement), a user is deemed to have consented to the ISP monitoring his or her emails and disclosing that information, if warranted, to law enforcement. In other words, that user waived his Fourth Amendment rights.

Courts have not yet addressed the issue, and so the question remains: given the lengthy, complicated and often confusing terms of a standard ISP service agreement, can a typical user of the internet be expected to understand that by agreeing to the terms of an ISP's service agreement, he or she is waiving an important constitutional right to privacy? Furthermore, even if the user does understand that by agreeing to use the ISP's service he or she is waiving Fourth Amendment protections, is there an alternative if all established mainstream ISPs require agreement to essentially the same terms of service?

Courts have considered the argument that "clickwrap" agreements meaning, agreements that are entered into by clicking "I Agree," (as is the case of ISPs' terms of service agreements) should be considered contracts of adhesion. A contract of adhesion is a standard form contract drafted by one party (usually a business with stronger bargaining power) and signed by the weaker party (usually a consumer in need of goods or services) who must adhere to the contract and does not have the power to negotiate or modify the terms of the contract. Courts use a higher level of scrutiny when determining the enforceability of contracts of adhesion.

Applying this standard, courts have found that (a) some clickwrap agreements are generally enforceable, but have invalidated the enforceability of certain terms contained in those

⁴ *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577 (1979).

⁵ *United States v. Jones*, 565 U.S. ___, 132 S. Ct. 945 (2012).

⁶ *United States v. DiTomasso*, No.: 14-cr-160 (SAS), 2014 WL 5462467 (SDNY October 28, 2014).

agreements, and also (b) some clickwrap agreements do not meet the criteria for enforceability of a unilateral form contract because certain terms of those clickwrap agreements are “unconscionable, and therefore unenforceable.”⁷

If you own or operate a business that utilizes the internet and an ISP (i.e., email, web browsers), it is important to take the necessary steps to protect your company’s information. Given the state of the law, care should be taken so that no email can be interpreted as a communication suggesting illegal activity, thus preserving your right to privacy as to all your emails. It is unclear how and whether an ISP’s right to review emails and share those emails with governmental authorities will expand beyond the realm of criminal communications, thereby creating the potential for loss of privacy even if no communication specifically suggests criminal activity. For that reason, it is not too early to consider adopting policies that will provide appropriate guidelines for employees regarding email content and communication on the internet.

Our Firm can assist you in drafting and implementing proper company policies and procedures, and advise you as to the most effective ways to protect your business. We will continue to monitor this issue and keep you advised of developments in this area.

Please contact Marc A. Lavaia, (212) 984-7740, mlavaia@wbcsk.com or your regular Warsaw Burstein LLP attorney for more information or to discuss questions you may have about your privacy rights.

Marc A. Lavaia

mlavaia@wbcsk.com

212-984-7740

Warsaw Burstein, LLP

© Warsaw Burstein, LLP, 2014. All rights reserved.

This memorandum was prepared as a service to clients and other friends of Warsaw Burstein to report on recent developments that may be of interest to them. The information in it is therefore general, and should not be considered or relied on as legal advice. Throughout this memorandum, "Warsaw Burstein" and the "firm" refer to Warsaw Burstein, LLP.

⁷ *Bragg v. Linden Research, Inc.*, 487 F.Supp.2d 593 (E.D. Pa. 2007).