Washington Journal of Law, Technology & Arts

Volume 5 | Issue 4 Article 4

3-1-2009

User Privacy and Information Disclosure: The Need for Clarity in "Opt-in" Questions for Consent to Share Personal Information

Suzanna Shaub

Corporate & Commercial
Cite as: Suzanna Shaub, *User Privacy and Information Disclosure: The Need for Clarity in "Opt-in" Questions for Consent to Share Personal Information*, 5 SHIDLER J. L. COM. & TECH. 18 (2009), *available at* <http://www.lctjournal.washington.edu/Vol5/a18Shaub.html>

USER PRIVACY AND INFORMATION DISCLOSURE: THE NEED FOR CLARITY IN "OPT-IN" QUESTIONS FOR CONSENT TO SHARE PERSONAL INFORMATION

Suzanna Shaub[1]

Abstract

Many company Web sites obtain permission to disclose their users' private information to third parties through the use of "opt-in" mechanisms, which require consumers to affirmatively grant consent to collect data from the user. These opt-in questions often ask general questions, such as whether the user would like to receive further information about the company or a product. Many companies construe an affirmative answer as consent to disclose personal information in accordance with its privacy policy. Although companies with this practice have generally avoided liability in the past, a recent case raises significant skepticism regarding the practice. In *CollegeNET, Inc. v. XAP Corp.*, a U.S. district court held that answering "yes" to an opt-in question may not qualify as express consent to disclose a user's private information. This Article addresses the potential causes of action, and likelihood of their success, against companies with these types of business practices. This Article also suggests that it is a good business practice to provide unambiguous opt-in questions to obtain informed consent from users before disclosing their personal information.

Table of Contents

INTRODUCTION

<1>"Are you interested in receiving information about student loans or financial aid?" This was the question an online college application service company asked its users to obtain consent to disclose the users' personal information to third parties.[2] A court has recently held, however, that genuine issues of material fact existed as to whether the users had actually provided express consent to disclose their personal information, and the plaintiffs were awarded $4.5 million dollars from the college application company at the subsequent trial.[3]

<2>Some of the largest U.S. companies currently use similarly ambiguous questions to collect and disclose their users' personal information. Companies often create opt-in questions asking whether the consumer would like more information about products or services, rather than a straightforward question. Such ambiguous mechanisms permit a Web site user to affirmatively grant the site consent before it collects information on the user. [4] A company then construes the consent granted to receive additional information to *also* mean that the consumer has affirmatively assented to information sharing. The opt-in questions all too often fail to either fully explain what the customer is consenting to, or direct the user to read the privacy policy.

<3>This Article discusses the potential causes of action available against companies using ambiguous opt-in questions, and suggests that such companies may be liable for their disclosures. The risk of liability is especially concerning in light of ever-expanding privacy concerns for consumers on the Internet. In addition, this Article argues that using ambiguous or vague opt-in questions is a poor business practice because it misleads users and exposes their personal information to third parties without fully obtaining informed consent.

POTENTIAL CAUSES OF ACTION AGAINST COMPANIES USING VAGUE OPT-IN QUESTIONS

<4>Legal protections available for an American's personal information are currently limited, despite the recent boom in privacy legislation in certain industries, including financial services and health care.[5] Both statutes and case law fall short

of clearly imposing liability on companies using ambiguous or vague opt-in questions prior to disclosing private information. Nevertheless, with ever-increasing concerns regarding protection of personal information on the Internet, courts may begin to expand the right to privacy to permit a cause of action against companies disclosing their visitors' private information without informed consent. Furthermore, courts may extend other common law doctrines, such as breach of contract, fraud, and negligence to prohibit such deceptive conduct.

Current Common Law Privacy Causes of Action and Their Weaknesses

<5>To succeed in a common law invasion of privacy claim, one must rely on one of the four following theories: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) misappropriation of name or likeness for commercial purposes; or (4) publicity that places another in false light.[6] However, the likelihood of success for an invasion of privacy claim on any of these theories is, at the present time, relatively low due to the difficulty of satisfying the legal elements of any of the aforementioned claims.[7] Indeed, this is especially true in the context of opt-in questions and the resulting Internet data collection and distribution.

<6>Each theory suffers substantial defects, which contribute to the improbability of a successful claim under any theory. For example, a claim under intrusion upon seclusion in an opt-in scenario would likely fail because the invasion upon another's physical seclusion or into their private affairs must be highly offensive or outrageous to a reasonable person.[8] Courts have not yet extended this doctrine to include Internet data collection, and have, in fact, held that digital intrusion is not such an offensive action where an individual could foresee their personal data being collected.[9] Similarly, courts have not yet extended the privacy theory of public disclosure of private facts to include Internet data gathering and distribution to third parties, and they appear unlikely to do so.[10]

<7>In addition, an invasion of privacy claim for misappropriation of name or likeness for commercial purposes offers few promises to consumers in this area. This is because it is not actually the users' unique or specific name or likeness that created the economic benefit, but rather the ability to sell users' personal information in general.[11] Furthermore, a cause of action under false light publicity would also be unlikely to support a claim of liability in the area of opt-in terms, as the doctrine requires publicizing information with knowledge of or

with reckless disregard for its falsity in a manner that would be highly offensive to a reasonable person.[12] Internet data collection and distribution does not fit this definition.[13] Nevertheless, where courts are unwilling to consider common law claims for breach of privacy or other common law theories of liability, the Federal Trade Commission Act may provide necessary support for a harmed consumer.

FEDERAL TRADE COMMISSION ACT AND COMPLIANCE WITH PRIVACY POLICIES

<8>The protection of online personal information in most U.S. industries is generally self-regulated, although companies often face liability if they fail to comply with their posted privacy policy.[14] Practically speaking, U.S. businesses must have a privacy policy in place because a large-market state—California—essentially mandated such an adoption in a 2003 statute.[15] The Federal Trade Commission (FTC), in addition to state Attorneys General, is often responsible for enforcement and compliance with posted privacy policies.[16]

<9>The FTC has interpreted the Federal Trade Commission Act (the "Act") as providing the FTC the authority to take action against companies that fail to follow the privacy policies posted on each respective Web site.[17] The FTC exercises its authority under Section 5 of the Act,[18] and Web site owners must follow their respective privacy policies regarding how information is gathered, maintained, used and protected to meet unfair and deceptive trade practices standards. In fact, in recent years, the FTC has taken administrative action against several companies that have breached their promises regarding how the company would have collected, stored, used and safeguarded personal information collected online.[19] The Commission has also pursued those that have suffered an inadvertent breach, in addition to pursuing companies that have made a material change in their privacy policy without notifying users.[20]

<10>For example, the FTC pursued administrative action against Guess?, Inc., a clothing manufacturer, for its failure to implement security measures that the company's posted privacy policy had promised were in place.[21] The FTC alleged that customer personal information was vulnerable to hackers, which was contrary to the privacy policy's assurances regarding the encryption of personal information.[22] The FTC argued, therefore, that the company violated Section 5 of the Act, because the privacy policy was false and misleading and the

clothing retailer's practices were unfair or deceptive. Guess?, Inc. ultimately settled the charges with the FTC.[24]

<11>In 2004, the FTC also claimed that Gateway Learning Corporation (Gateway), which markets and sells "Hooked on Phonics," had violated its privacy policy.[25] The FTC asserted that Gateway violated its own terms in collecting its users' information and then, without notice or consent, altering its privacy policy to allow for third party disclosure.[26] Gateway ultimately settled with the FTC for renting its users' personal information to marketers, which was an act in contravention of the nondisclosure assurances found in the privacy policy.[27]

<12>Because the Act does not expressly provide for a private cause of action, nor has any federal court implied that such an action is available,[28] enforcement actions regarding privacy policy compliance are relatively rare and are often settled. However, companies clearly face liability from the FTC under to the Act for failing to comply with their internal privacy policies.[29] Furthermore, the FTC could potentially find non-compliance with the Act if the Commission deems the applicable opt-in question to be too vague or ambiguous, or to fail to provide users adequate notice of their disclosure practices. Where the Federal Trade Commission Act is inapplicable, however, the Lanham Act may provide a potential cause of action for a harmed consumer.

FALSE ADVERTISING UNDER THE LANHAM ACT

<13>The Lanham Act may also supply a potentially successful cause of action against companies with vague or misleading opt-in questions. In general, the Lanham Act prohibits misrepresenting the nature, qualities, or characteristics of goods, services, or commercial activities through false advertising or similar activities.[30] Any person who believes he or she is or is likely to be damaged by this misrepresentation can file a claim under the Lanham Act.[31] To prove a false advertising claim under the Lanham Act, the plaintiff must establish the following elements: (1) that the defendant made a false statement of fact about its own or another's product in a commercial advertisement; (2) that the statement actually deceived or had the tendency to deceive a substantial segment of the defendant's audience; (3) that the deception is material, in that it is likely to influence the purchasing decision; (4) that the defendant caused its falsely advertised product to enter interstate commerce; and (5) that the plaintiff has been or is likely to be injured as the result of the false statement either by

direct diversion of sales from itself to defendant, or by lessening of the goodwill which its products enjoy with the buying public.[32]

<14>In a legal battle between competitors, the court in *CollegeNET, Inc. v. XAP Corp.* found liability under the Lanham Act for an ambiguous opt-in question. The *CollegeNET* Court held that genuine issues of material fact existed as to whether the users had actually provided express consent to disclose user personal information, and the jury in the subsequent federal trial awarded $4.5 million in damages to the competitor upon finding the opt-in question was unclear and, therefore, deceptive.[33] More specifically, both parties in *CollegeNET* provided online college admission application services to the prospective students, and colleges and universities to which the students would apply.[34] The plaintiff, CollegeNET, Inc. (CollegeNET), charged colleges a fee for its service, while the defendant, XAP Corporation (XAP), did not.[35] Rather, in the case of XAP, state agencies, departments of education, banks and other lending institutions paid the company in exchange for information regarding the students' personal data.[36]

<15>XAP's privacy policy stated that it would not release personal consumer data without the user's express consent.[37] However, XAP disclosed such information after a user responded "yes" to the general opt-in question, "Are you interested in receiving information about student loans or financial aid?"[38] CollegeNET then sued XAP under the Lanham Act for unfair competition, asserting the following claims: (1) making false representations to its consumers regarding its privacy policy; and (2) breach of confidentiality regarding its users' personal information.[39] CollegeNET contended that XAP's allegedly false privacy policy statement and false representations induced students to provide personal information, and that this practice placed CollegeNET at an unfair disadvantage because XAP is able to provide its services free of charge.[40] In turn, XAP earned money by selling this information to commercial institutions.

<16>*CollegeNET* is a significant case because it provides an example of a company's potential liability for false advertising for using ambiguous opt-in questions to obtain consent from its users. The large judgment of $4.5 million dollars should alert companies that they could face potential liability under the Lanham Act for unclear opt-in questions. However, the significance of this case for consumers is undermined by the fact that it was brought under the Lanham Act, and not under a privacy invasion tort theory. Courts generally hold that standing

under the false advertising prong of the Lanham Act is limited to direct competitors of the advertiser.[41] Neither individual consumers, classes of consumers, nor organizations representing consumers have standing under the Lanham Act for a false advertising suit.[42] As such, companies with vague opt-in questions should be concerned over the *CollegeNET* ruling only to the extent to which there is a substantial likelihood that a competitor will sue, and can satisfy the Lanham Act requirements. These requirements may be difficult to meet, as the plaintiff must prove the defendant's false privacy policy actually deceived its customers, which injured or is likely to injure the plaintiff's business as a result.[43] Even without standing or the availability of a Lanham Act claim, additional contractual issues may also be relevant.

GIVING NOTICE: CONTRACT FORMATION AND OPT-IN QUESTIONS

<17>When companies provide opt-in questions requesting a user's consent, the company should ensure that the user has manifested his or her consent to the disclosure agreement's terms to form a binding contract. Although an affirmative answer to an opt-in question is, in general, a manifestation of the user's consent to the terms,[44] courts have held that a privacy statement, without more, does not necessarily form a unilateral contract binding the parties.[45] In the case *In re Northwest Airlines Privacy Litigation*, for example, the defendant Northwest Airlines successfully contended that its posted privacy policy did not form a binding contract between the company and its customers, and, therefore, did not breach its contract when it violated the terms of its privacy policy.[46]

<18>A court could, nevertheless, hold that a user's acceptance of a Web site's privacy policy is invalid if the consumer is not properly informed. In *Register.Com, Inc. v. Verio, Inc.*, for example, the defendant argued that there was no icon to click to indicate assent to the plaintiff's terms, so the terms did not bind him.[47] The court rejected this argument, however, stating that by submitting a query to the site, the defendant manifested acceptance of the clearly posted terms of use forming a binding contract. Despite this holding, cases such as *Register.Com, Inc. v. Verio, Inc.* should, however, stress the importance of clearly posting privacy policy terms to ensure disclosure agreement enforcement.

CONCLUSION

<19>Due to ever-increasing concerns regarding privacy law and

the collection and dissemination of information collected on the Internet, courts may be more open to imposing liability upon companies obtaining consent through vague opt-in questions. Both federal statutes and common law theories, such as invasion of privacy and contract formation issues, provide courts with the tools to do so. Specifically, this legal risk is evident in CollegeNET, in which the court held that an affirmative response to an opt-in question might not provide express consent for companies to disclose personal consumer information to third parties. As such, companies should consider implementing the following Practice Pointers to comply with sound business practices and possible developments in the applicable law.

PRACTICE POINTERS

- Implement a privacy policy governing the collection, use, storage, and dissemination of personal information collected from users.
- Inform customers of applicable privacy policy sections in order to obtain express and informed consent to disclose personal information to third parties.
- Provide sufficient information in opt-in questions, such as, "By clicking 'yes', you are providing us permission to disclose your information to third parties."
- Avoid opt-in questions with a pre-checked default answer, as it raises questions whether the user's consent was actually express.
- When collecting and disclosing users' personal information, have policies in place verifying that third parties are using that information in approved manners.
- Implement a procedure that will permit users to withdraw their consent or opt-out of information gathering and disclosure.

<< Top

Footnotes

1. Suzanna Shaub, University of Washington School of Law, J.D. program Class of 2008. Thank you to Professor Jane Winn of the University of Washington School of Law, and Jared Barrett for their guidance

and feedback on this Article. Thank you also to Chris Jay Hoofnagle, Director of the Berkeley Center for Law and Technology's information privacy programs and Senior Fellow to the Samuelson Law, Technology, and Public Policy Clinic.

2. CollegeNET, Inc. v. XAP Corp., 442 F. Supp. 2d 1070, 1072 (D. Or. 2006).

3. *Id.* at 1076; CollegeNET, Inc. v. XAP Corp., 483 F. Supp. 2d 1058, 1061 (D. Or. 2007).

4. Shaun A. Sparks, *The Direct Marketing Model and Virtual Identity: Why the United States Should Not Create Legislative Controls on the Use of Online Consumer Personal Data*, 18 DICK. J. INT'L L. 517, 527 (2000).

5. JANE K. WINN & BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE § 14.01 (4th ed., Aspen L. & Bus. 2001 & Supp. 2007); Health Insurance Portability and Accountability Act § 264, 42 U.S.C. § 1320d-1(a) (2006).

6. *Id.* at 837; RESTATEMENT (SECOND) OF TORTS § 652A (1977).

7. Brian Keith Groemminger, Note, *Personal Privacy on the Internet: Should It Be a Cyberspace Entitlement?*, 36 IND. L. REV. 827, 837 (2003).

8. Groemminger, *supra* note 7, at 837; RESTATEMENT (SECOND) OF TORTS § 652B (1977).

9. Groemminger, *supra* note 7, at 837.

10. *Id.*

11. WINN & WRIGHT, *supra* note 5, § 14.03[B] (citing RESTATEMENT (SECOND) OF TORTS § 652C (1977)).

12. RESTATEMENT (SECOND) OF TORTS § 652E (1977).

13. Groemminger, *supra* note 7, at 837-38.

14. WINN & WRIGHT, *supra* note 5, § 14.01.

15. WINN & WRIGHT, *supra* note 5, § 14.07[C] (citing CAL. CIV. CODE §§ 1798.29, 1798.82 (2003)).

16. JANE K. WINN & BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE § 14.01 (4th ed., Aspen L. & Bus. 2001 & Supp. 2005).

17. Federal Trade Commission Act §5, 15 U.S.C. § 45

(2006); WINN & WRIGHT, *supra* note 5, §14.03[O].

18. Fed. Trade Comm'n, Enforcing Privacy Promises: Section 5 of the FTCA, http://www.ftc.gov/privacy/privacyinitiatives/promises.html (last visited Nov. 5, 2009).

19. *See generally* MARCIA HOFMANN, *The Federal Trade Commission's Enforcement of Privacy*, *in* PROSKAUER ON PRIVACY (2006).

20. *Id.*

21. Press Release, Fed. Trade Comm'n, Guess Settles FTC Security Charges; Third FTC Case Targets False Claims About Information Security (June 18, 2003), http://www.ftc.gov/opa/2003/06/guess.htm.

22. *In re* Guess?, Inc., 136 F.T.C. 507, 509-10 (2003).

23. *Id.* at 513.

24. *Id.* at 527-28.

25. Press Release, Fed. Trade Comm'n, Gateway Learning Settles FTC Charges (July 7, 2004), http://www.ftc.gov/opa/2004/07/gateway.shtm.

26. *Id.*

27. *Id.*

28. Jackson v. R. G. Whipple, Inc., 627 A.2d 374, 384 n.14 (Conn. 1993) (citing Am. Airlines v. Christensen, 967 F.2d 410 (10th Cir. 1992)).

29. WINN & WRIGHT, *supra* note 5, at §14.01.

30. The statute provides the following relevant language: "[a]ny person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which—(A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or (B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his

or her or another person's goods, services, or commercial activities, shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act." Lanham Act § 43(a), 15 U.S.C. § 1125(a)(1) (2006).

31. *Id*.

32. *CollegeNET, Inc.*, 442 F. Supp. 2d 1070, 1075 (D. Or. 2006).

33. *Id.* at 1076; CollegeNET, Inc. v. XAP Corp., 483 F. Supp. 2d 1058, 1061 (D. Or. 2007).

34. *CollegeNET, Inc.*, 442 F. Supp. 2d at 1072.

35. *Id.* at 1074.

36. *Id.* at 1072.

37. *Id.*

38. *Id.* at 1072-73.

39. *CollegeNET, Inc.*, 442 F. Supp. 2d at 1074.

40. *Id.* at 1076.

41. *Compare* Jack Russell Terrier Network of N. Cal. v. Am. Kennel Club, Inc., 407 F.3d 1027, 1037 (9th Cir. 2005) (affirming that standing under the false advertising prong of § 43a is limited to direct competitors of the advertiser), *with* Ortho Pharm. Co. v. Cosprophar, Inc., 32 F.3d 690, 694 (2d Cir. 1994) (observing that to have standing to sue for false advertising under the Lanham Act, a plaintiff "need not demonstrate that it is in direct competition with the defendant . . . .").

42. Barrus v. Sylvania, 55 F.3d 468, 470 (9th Cir. 1995); Serbin v. Zeibart Int'l Corp., 11 F.3d 1163, 1177 (3d Cir. 1993).

43. *Serbin*, 11 F.3d at 1175.

44. *See* Cairo, Inc. v. Crossmedia Servs., No. C 04-04825 JW, 2005 U.S. Dist. LEXIS 8450 (N.D. Cal. 2005) (indicating the defendant's "Terms of Use" were enforceable against the plaintiff where the plaintiff did not explicitly agree to the Terms, but its visits to the Web site with knowledge of the "Terms of Use" constituted acceptance of them); *see also* Register.com v. Verio, Inc., 126 F. Supp. 2d 238, 248 (S.D.N.Y. 2000).

45. *See In re* Nw. Airlines Privacy Litig., No. Civ. 04-126, 2004 U.S. Dist. LEXIS 10580, at *15 (D. Minn. June 6, 2004) (holding dismissal was appropriate after Northwest Airlines disclosed electronic passenger records, including their flight numbers, credit card data, traveling companions, and related travel reservations to NASA.).

46. *Id.*

47. *Register.com*, 126 F. Supp. 2d at 248.