Berkeley Technology Law Journal

Volume 30 | Issue 1 Article 3

Spring 3-1-2014

Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding

Joel R. Reidenberg

Travis Breaux

Lorrie Faith Carnor

Brian French

Link to publisher version (DOI)
https://doi.org/10.15779/Z384K33

DISAGREEABLE PRIVACY POLICIES: MISMATCHES BETWEEN MEANING AND USERS' UNDERSTANDING†

Joel R. Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T. Graves, Fei Liu, Aleecia McDonald, Thomas B. Norton, Rohan Ramanath, N. Cameron Russell, Norman Sadeh and Florian Schaub††

ABSTRACT

Privacy policies are verbose, difficult to understand, take too long to read, and may be the least-read items on most websites even as users express growing concerns about information collection practices. For all their faults, though, privacy policies remain the single most important source of information for users to attempt to learn how companies collect, use, and share data. Likewise, these policies form the basis for the self-regulatory notice and choice framework that is designed and promoted as a replacement for regulation. The underlying value and legitimacy of notice and choice depends, however, on the ability of users to understand privacy policies.

This paper investigates the differences in interpretation among expert, knowledgeable, and typical users and explores whether these groups can understand the practices described in privacy policies at a level sufficient to support rational decision-making. This paper seeks

---

† For their comments on this study, the authors would like to acknowledge and thank Alessandro Acquisti, Noah A. Smith, and Shomir Wilson, and the participants at the 2014 TPRC 42nd Research Conference on Communication, Information and Internet Policy. Funding for this project was provided, in part, by the National Science Foundation under its Secure and Trustworthy Computing (SaTC) initiative grants 1330596, 1330214, and 1330141 for "TWC SBE: Option: Frontier: Collaborative: Towards Effective Web Privacy Notice and Choice: A Multi-Disciplinary Prospective" and by a Fordham Law School Faculty Research Grant.

†† Respectively, Stanley D. and Nikki Waxberg Chair and Professor of Law, Fordham University; Assistant Professor of Computer Science, Carnegie Mellon University; Professor of Computer Science and Engineering & Public Policy, Carnegie Mellon University: Senior Research Programmer, Carnegie Mellon University; Research Fellow, Fordham Center on Law and Information Policy; Ph.D Candidate (Engineering and Public Policy) Carnegie Mellon University; Ph.D Candidate (Computer Science), Carnegie Mellon University; Director of Privacy, Stanford Center for Internet & Society; Privacy Fellow, Fordham Center on Law and Information Policy; Masters Candidate (Computer Science), Carnegie Mellon University; Executive Director, Fordham Center on Law and Information Policy; Professor of Computer Science, Carnegie Mellon University; Postdoctoral Fellow (Computer Science), Carnegie Mellon University.

to fill an important gap in the understanding of privacy policies through primary research on user interpretation and to inform the development of technologies combining natural language processing, machine learning, and crowdsourcing for policy interpretation and summarization.

For this research, we recruited a group of law and public policy graduate students at Fordham University, Carnegie Mellon University, and the University of Pittsburgh ("knowledgeable users") and presented these law and policy researchers with a set of privacy policies from companies in the e-commerce and news and entertainment industries. We asked them nine basic questions about the policies' statements regarding data collection, data use, and retention. We then presented the same set of policies to a group of privacy experts and to a group of crowd workers representing typical Internet users.

The findings show areas of common understanding across all groups for certain data collection and deletion practices, but also demonstrate very important discrepancies in the interpretation of privacy policy language, particularly with respect to data sharing. The discordant interpretations arose both within groups and between the experts and the two other groups.

The presence of these significant discrepancies has critical implications. First, the common understandings of some attributes of described data practices mean that semi-automated extraction of meaning from website privacy policies may be able to assist typical users and improve the effectiveness of notice by conveying the true meaning of these policies. However, the disagreements among experts and disagreement between experts and the other groups reflect that ambiguous wording in typical privacy policies undermines the ability of privacy policies to effectively convey notice of data practices to the general public.

The results of this research will, consequently, have significant policy implications for the construction of the notice and choice framework and for the U.S. reliance on this approach. The gap in interpretation indicates that privacy policies may be misleading the general public and that those policies could be considered legally unfair and deceptive. And, where websites are not effectively conveying privacy policies to consumers in a way that a "reasonable person" could, in fact, understand the policies, "notice and choice" fails as a framework. Such a failure has broad international implications since websites extend their reach beyond the United States.

TABLE OF CONTENTS

I. INTRODUCTION

Privacy policies are verbose, difficult to understand, take too long to read, and may be the least-read items on most websites even as users express growing concerns about information collection practices. But, for all their faults, privacy policies remain the single most important source of information for users to attempt to learn how companies collect, use, and share data. The reason that privacy policies are so important is that the United States takes a "notice and choice" approach to Internet privacy.[1] The idea is that companies post their privacy policies, users read and understand these policies, and then users follow a rational decision-making process to engage only with companies they believe offer an acceptable level of privacy. This structure is designed and promoted as a replacement

1. *See infra* Section II.A.

for regulation. The underlying value and legitimacy of notice and choice thus depends on the ability of users to understand privacy policies.

This paper investigates whether expert, knowledgeable, and typical users can understand the practices described in privacy policies at a level sufficient to support rational decision-making. The paper seeks to fill an important gap in the understanding of privacy policies of typical users through primary research on user interpretation. This research can inform the development of natural language processing and crowdsourcing for policy interpretation and summarization.[2] Part II of the paper discusses the existing landscape for notice and choice policies and the gaps in prior research on user understanding. Part III then defines the methodology used for the research. Part IV presents the results and reports on discrepancies in the interpretation of privacy policy language among three different groups: privacy experts, law and policy graduate students, and typical users. These results reveal significant discrepancies across the groups. Part V analyzes the critical implications of these discrepancies.

The results of this research will, consequently, have significant policy implications for the construction of the notice and choice framework and for the U.S. reliance on this approach. The implications also expand beyond the United States since websites extend their reach globally.

II. THE LANDSCAPE

This Part will first explain how and why notice and choice is used as a mechanism to address privacy protection. In the United States, notice and choice has become the principal means to address privacy online. While

2. *See* Norman Sadeh et al., Towards Usable Privacy Policies: Semi-automatically Extracting Data Practices From Websites' Privacy Policies (2014) (poster, ACM Symposium on Usable Security and Privacy (SOUPS)), *available at* https://cups.cs.cmu.edu/soups/2014/posters/soups2014_posters-paper20.pdf; NORMAN SADEH ET AL., THE USABLE PRIVACY POLICY PROJECT: COMBINING CROWDSOURCING, MACHINE LEARNING AND NATURAL LANGUAGE PROCESSING TO SEMI-AUTOMATICALLY ANSWER THOSE PRIVACY QUESTIONS USERS CARE ABOUT (Carnegie Mellon Univ., Sch. of Computer Sci., Inst. for Software Research Technical Report No. CMU-ISR-13-119, Dec. 2013), *available at* http://reports-archive.adm.cs.cmu.edu/anon/isr2013/abstracts/13-119.html; Steve Bellovin & Sebastian Zimmeck, *Machine Learning Analysis of Privacy Policies*, MICH. TELECOMM. & TECH. L. REV. (forthcoming 2014); Sebastian Zimmeck & Steven M. Bellovin, *Privee: An Architecture for Automatically Analyzing Web Privacy Policies*, *in* PROCEEDINGS OF THE 23RD USENIX SECURITY SMPOSIUM (Aug. 2014), *available at* https://www.usenix.org/conference/usenixsecurity14/technicalsessions/presentation/zimmeck.

more extensive regulation exists in Europe,[3] notice and choice on an international scale plays important roles in the assurance of both privacy rights and international data flows. The implementation of notice and choice in the United States is also affected by the international presence of U.S. websites.

For notice and choice to work effectively, notice must be meaningful for users. This Part will also address prior research into the usability of privacy policies, describe usability problems, and, thus, reveal the gap to be filled by this research.

A. THE NOTICE AND CHOICE FRAMEWORK

Since the 1970s, the United States has promoted fair information practice standards as the guidepost for the protection of privacy.[4] These principles appear in U.S. law, but the U.S. legal system shies away from comprehensive privacy regulation.[5] Historically, the United States has addressed discrete privacy issues in narrow statutes, which have been targeted to specific problems and focused on specific actors.[6] Over the years, the White House, Congress, and the Federal Trade Commission ("FTC") have encouraged private sector responses to privacy challenges in lieu of new regulation.[7]

Notice and choice are the critical elements for self-regulation of fair information practices. "Notice" is generally described in terms of transparency of the information practices. The FTC has stated the principle as giving

---

3. *See* Directive 95/46 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, 1995 O.J. (L 281) (EC).

4. *See* Robert Gellman, *Fair Information Practices: A Basic History* (Aug. 3, 2014), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

5. *See, e.g.*, PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996).

6. *See, e.g.*, Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195 (1992); SCHWARTZ & REIDENBERG, *supra* note 5.

7. *See, e.g.*, WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (Feb. 23, 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (voluntary approach); THE PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (July 1977); FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998), *available at* http://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/priv-23a_0.pdf [hereinafter PRIVACY ONLINE]; U.S. DEP'T OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE at viii (June 12, 1997), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

> consumers . . . notice of an entity's information practices before any personal information is collected from them . . . . [N]otice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:
>
> - identification of the entity collecting the data;
> - identification of the uses to which the data will be put;
> - identification of any potential recipients of the data;
> - the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);
> - -whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and
> - -the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.[8]

Adequate and meaningful notice is necessary for users to be able to make informed decisions about their privacy choices.

"Choice" is typically defined in terms of consent. As the FTC articulates: "[a]t its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information—*i.e.*, uses beyond those necessary to complete the contemplated transaction."[9]

Combined, notice and choice are used as a fundamental aspect of privacy protection in the private sector.

Notice and choice is also an important part of the international framework for transborder data flows. In 2000, the European Union and the United States adopted the Safe Harbor agreement to facilitate international data flows.[10] Under the voluntary agreement, U.S. companies would agree to seven principles that were designed to assure the privacy of their E.U. origin

8. *See* PRIVACY ONLINE, *supra* note 7, at 7–8.

9. *Id.* at 8.

10. *See* U.S. DEP'T OF COMMERCE, SAFE HARBOR PRIVACY PRINCIPLES (Jul. 21, 2000), *available at* http://export.gov/safeharbor/eu/eg_main_018475.asp [hereinafter SAFE HARBOR PRINCIPLES]; Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717 (2001).

data. The Safe Harbor agreement specifically included "notice" and "choice" as two essential principles.[11]

The "notice" principle required website operators to "inform individuals about the purposes for which it collects and uses information about them" in "clear and conspicuous language."[12] The "choice" principle added that those organizations and companies collecting personal information were required to "offer individuals the opportunity to choose (opt out [of]) whether their personal information [was] (a) to be disclosed to a . . . third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected."[13] Like the notice principle, "choice" demanded that companies construe their privacy agreements with clarity, stating that "[i]ndividuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice."[14]

The global reach of U.S. websites and the impact of foreign standards on American website practices makes the international importance of notice and choice quite high. Similar to the American doctrine, the Article 29 Working Party of European data protection commissioners has looked to notice and choice in a number of initiatives to protect personal data. For example, in 2013, the Working Party released a guidance document for website operators on obtaining website users' consent for the use of tracking cookies.[15] The Working Party specified that to provide sufficient notice, websites must provide users with specific information about how and why they used cookies.[16] Attaining users' "blanket consent" without first supplying exact facts would not suffice.[17] The Working Party suggested that website operators configure browsers to require users to actively signify their consent and leave no doubt as to the users' subjective intent.[18] Moreover, the Working Party emphasized that users be offered a free choice regarding the use of tracking cookies and that users be able to browse a website while declining cookies.[19] The Italian Data Protection Authority internalized the

11. *See* SAFE HARBOR PRINCIPLES, *supra* note 10.
12. *See id.*
13. *See id.*
14. *See id.*
15. *See Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies,* The European Commission Article 29 Working Party (adopted Oct. 2, 2013), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf.
16. *Id.* at 3.
17. *Id.*
18. *Id.*
19. *Id.* at 5.

Working Party's guidance in May of 2014.[20] Among its resolutions was that website banners should contain clear and visible notice and consent requests for users.[21]

Though many of the Working Party's initiatives adopted notice and choice principles, the E.U. data protection authorities also recognize the limitations of notice and choice. At the Safe Harbor Conference in 2009, Dutch Data Protection Authority chairman Jacob Kohnstamm stated in his introductory remarks that enforcement tools (e.g., fines) may be a superior means of ensuring the protection of website users' personal data.[22] Kohnstamm stated that "[d]ue to new technological applications[,] transparency alone [notice and choice] is no longer sufficient to guarantee that individuals can oversee the consequences of data processing activities . . . independent oversight is necessary. It is necessary to ensure a level playing field. To ensure that all are abiding to the same rules."[23] In essence, Kohnstamm was expressing important skepticism about the ability for notice and choice to effectively protect individual privacy.

B. RESEARCH ON USABILITY AND TECHNICAL TOOLS

Prior research has shown that the terms contained in policies are frequently unfamiliar to users, and the level of education necessary to understand the policies is high.[24] Similarly, research has also shown that notice of privacy policies may not be effective and that some notices are designed to nudge users into disclosing larger quantities of personal information than necessary for the interaction.[25] Privacy technologists have

20. *See* THE ITALIAN DATA PROTECTION AUTHORITY, SIMPLIFIED ARRANGEMENTS TO PROVIDE INFORMATION AND OBTAIN CONSENT REGARDING COOKIES (May 8, 2014), *available at* http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167654.

21. *Id.* at 3.

22. Jacob Kohnstamm, Chairman, Dutch Data Protection Authority, Introductory Speech at the Safe Harbor Conference in Washington (2009), *available at* http://www.dutchdpa.nl/downloads_int/20091118_speech_jko_washington.pdf.

23. *Id.* at 8.

24. *See* Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Notices*, PRIVACY RIGHTS CLEARINGHOUSE (July 1, 2001), https://www.privacyrights.org/ar/GLB-Reading.htm ("Readability analysis of . . . privacy notices found that they are written at a 3rd-4th year college reading level, instead of the junior high school level that is recommended for materials written for the general public"); Mark A. Graber, Donna M. D'Alessandro & Jill Johnson-West, *Reading Level of Privacy Policies on Internet Health Web Sites*, 51 J. OF FAM. PRAC. 642, 642 (2002), *available at* http://www.jfponline.com/fileadmin/jfp_archive/pdf/5107/5107JFP_BriefReport.pdf (noting that healthcare websites that contain privacy statements are beyond the reading level of most adults).

25. *See* Yang Wang et al., *From Facebook Regrets to Facebook Privacy Nudges*, 74 OHIO ST. L.J. 1307 (2013).

developed tools to facilitate notice and choice for online users, but they have achieved only limited success.

1. Usability

Previous work has shown that while users have difficulty finding and using privacy policy information, they remain interested in this information, and when this information is made salient it can impact users' online purchasing decisions.[26] Research has also demonstrated that users are interested in several different pieces of information found in privacy policies.[27] This suggests that the information in privacy policies could be helpful if presented in a usable way.

Prior research also found that expecting users to read privacy policies places an unreasonably high burden on them because policies take so long to read.[28] As a result, there have been several approaches to improving usability. One approach to making privacy policies more accessible is a privacy "nutrition label" that summarizes key points from a privacy policy in a succinct and standard form.[29] While this approach has shown promise in research studies, it has not yet been widely adopted.[30]

---

26. Janice Y. Tsai, Serge Egelman, Lorrie Cranor & Alessandro Acquisti, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RESEARCH 254 (JUN. 2011), *available at* http://pubsonline.informs.org/doi/pdf/10.1287/isre.1090.0260 (study participants tended to purchase from online retailers who respected their privacy). For the use of default settings to prompt users to both disclose or share personal information, *see* Issac Dinner, Eric J. Johnson, Daniel G. Goldstein & Kaiya Liu, *Partitioning Default Effects: Why People Choose Not to Choose*, 17 J. EXPERIMENTAL PSYCHOL.: APPLIED 432 (2011); Daniel Goldstein et al., *Nudge Your Customers Toward Better Choices*, 86 HARV. BUS. REV. 12, 99–105 (2008). For a discussion of changes to Facebook's interface that promote sharing, see Fred Stutzman, Ralph Gross & Alessandro Acquisti, *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4 J. PRIVACY & CONFIDENTIALITY 7 (2012).

27. *See* Pedro G. Leon et al., *What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers*, *in* PROCEEDINGS OF THE EIGHTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY (SOUPS) (2013), *available at* http://cups.cs.cmu.edu/soups/2013/proceedings/a7_Leon.pdf; Jialiu Lin et al., *Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings*, *in* PROCEEDINGS OF THE ACM SYMPOSIUM ON USABLE SECURITY AND PRIVACY (SOUPS) (July 2014) (quantifying users' willingness to disclose or grant different mobile app privacy permissions—"different pieces of information found in privacy policies").

28. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J. L. & POL'Y 540 (2008).

29. Patrick G. Kelley et al., *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, CYLAB (Jan. 12, 2010), http://www.cylab.cmu.edu/research/techreports/2009/tr_cylab09014.html.

30. *Id.*

Layered privacy notices are another approach. Layered notices present a website's privacy policy to users in multiple "layers," with each describing elements of the policy in greater levels of detail and specificity.[31] Typically, these notices consist of a "short notice in a common template format" coupled with a "longer complete notice."[32]

Proponents of this approach advocate that layered notices "easily build consumer trust" and "increase public understanding of privacy and data protection" because the notices are "easy to read and understand."[33] One study revealed, however, that though layered notices enabled study participants to make decisions more quickly, the participants often responded inaccurately to questions about terms they had read in the notices.[34] Furthermore, the results suggested that participants rarely probed beyond the initial layer, thus leaving them with "incorrect impressions" of the privacy practices described by the more-complete policy.[35]

2. Technical Tools

Privacy technologists have also developed a variety of tools for users to express privacy preferences and for users to opt out of receiving targeted ads. However, the evaluation and deployment of these technologies over the years shows that the challenges to building effective tools have not been overcome. These challenges include the imposition of burdens on users to understand complex and diverse privacy preferences[36] and to comprehend

---

31. *See* CTR. FOR INFO. POLICY LEADERSHIP, TEN STEPS TO DEVELOP A MULTILAYERED PRIVACY NOTICE 1 (Mar. 2007), *available at http:*//www.informationpolicycentre.com/files/Uploads/Documents/Centre/Ten_Steps_whitepaper.pdf.

32. *Id.* at 1. This guide proposes that notices contain three layers:

> Layer 1 - The short notice: the very minimum, for example, when space is very limited, providing only the identity of the data controller, contact details, and the purposes of processing.
> Layer 2 - The condensed notice: covering the basics in less than a page, ideally using subheadings, and covering Scope; Personal information collected; Uses and sharing; Choices (including any access options); Important information; How to contact us.
> Layer 3 - The full notice.

Id. at 2–3.

33. *Id.* at 3–4.

34. *See generally* ALEECIA M. MCDONALD ET AL., *A Comparative Study of Online Privacy Policies and Formats*, *in* PRIVACY ENHANCING TECHNOLOGIES 37 (Aug. 2009), *available at* http://robreeder.com/pubs/PETS2009.pdf.

35. *Id.* at § 6.

36. *See, e.g.*, Michael Benisch et al., *Capturing Location-Privacy Preferences: Quantifying Accuracy and User-Burden Tradeoffs*, 15 J. PERSONAL & UBIQUITOUS COMPUTING 7 (Oct. 2011), *available at* http://www.normsadeh.com/file_download/142.

general usability features such as mechanisms to opt out in the context of online behavioral advertising.[37] These challenges emerge from the most prominent technical efforts to address notice and choice.

a) P3P

Growing concern by Congress and threats from the FTC to regulate online privacy gave rise to the Platform for Privacy Preferences ("P3P")—a web standard developed by the World Wide Web Consortium ("W3C") that enables web browsers to read website privacy policies automatically and compare them with user-specified privacy preferences.[38] Essentially, P3P would enable users to avoid websites whose practices did not meet their privacy preferences.[39] P3P specification 1.0 was launched in 2002.[40] Though a more developed specification 1.1 working draft was later produced, it was never finalized, as the W3C's working group "closed . . . due to lack of industry participation" in 2006.[41]

While some popular web browsers have integrated P3P tools,[42] others have not.[43] Furthermore, the users of browsers that have integrated P3P are reportedly unaware of the tool.[44] In addition, thousands of websites that adopted P3P appear to have used P3P codes to circumvent browser cookie blocking, without making accurate computer-readable statements about their

37. Pedro Leon et al., *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising*, *in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 589–98 (2012), *available at* http://dl.acm.org/citation.cfm?doid=2207676.2207759; Pedro Giovanni Leon et al., *What Do Online Behavioral Advertising Privacy Disclosures Communicate to Users?*, *in* PROCEEDINGS OF THE ACM WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY (WPES) 19–30 (2012), *available at* http://doi.acm.org/10.1145/2381966.2381970.

38. *See* Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. ON TELECOMM. & HIGH TECH. L. 273, 279 (2012).

39. *Id. See also* Kimberly Rose Goldberg, Note, *Platform for Privacy Preferences ("P3P"): Finding Consumer Assent to Electronic Privacy Policies*, 14 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 255 (2003).

40. *See* Cranor, *supra* note 38, at 279.

41. Cranor, *supra* note 38, at 280.

42. Namely, Microsoft Internet Explorer 6, 7, 8, and 9. *See* Cranor, *supra* note 38, at 280.

43. Neither Firefox, Safari, nor Chrome have integrated P3P, though "a number of prototype plug-ins and extensions," "authoring tools," and "prototype P3P user agents" have been developed. *See* Cranor, *supra* note 38, at 280–81.

44. Cranor asserts, "While I know of no formal studies, my informal polls of hundreds of audience members at talks I have given suggests that outside of groups of privacy experts, almost nobody has heard of P3P . . . ." Cranor, *supra* note 38, at 281.

privacy policies.[45] Thus, P3P policies have become an unreliable source of privacy policy information.

b) Do Not Track

In 2007, privacy advocates began discussing the creation of a mechanism that would enable users to register their opposition to being tracked online. The mechanism would be similar to the "Do Not Call" list for opting out of telemarketing solicitations.[46] Over time, this idea developed into a technical mechanism that would allow user agents—including web browsers, cell phones, email clients, and anti-malware packages—to send a "do not track" signal on the user's behalf.[47] In 2010, a Federal Trade Commission report requested comments on the idea of Do Not Track ("DNT").[48]

DNT similarly became a popular topic with legislators. Multiple bills at both the state and federal levels would have made DNT a legal requirement, but only one passed into law: California's AB 370.[49] Under AB 370, companies with customers who are California citizens must disclose how, if at all, they respond to an incoming DNT request.[50] In practice, this disclosure requirement is a de facto national (and international) standard, since most English language websites will likely have at least one visitor from California.[51]

By 2012, all major web browsers had implemented an interface for users to send a DNT request. However, the implementation of DNT remains elusive. While DNT is a promising idea, there are three major barriers to

45. PEDRO GIOVANNI ET AL., *Token Attempt: The Misrepresentation of Website Privacy Policies Through the Misuse of P3P Compact Policy Tokens*, *in* WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY (WPES) 4 (Oct. 2010), *available at* https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab10014.pdf.

46. Christopher Soghoian, *The History of the Do Not Track Header*, SLIGHT PARANOIA (Jan. 21, 2011), http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html.

47. DONOTTRACK.US, http://donottrack.us/ (last visited May 19, 2015); J. Mayer et al., *Do Not Track: A Universal Third-Party Web Tracking Opt Out*, INTERNET ENGINEERING TASK FORCE (Mar. 7, 2011), http://tools.ietf.org/html/draft-mayer-do-not-track-00/.

48. FED. TRADE COMM'N, A PRELIMINARY FTC STAFF REPORT ON PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS A-4 (December 1, 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

49. Assemb. 370, Ch. 390, Reg. Sess. (Cal. 2013) (amending CAL. BUS. & PROF. CODE § 22575), *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB370.

50. *Id.* at § 1(b)(5) (amending CAL. BUS. & PROF. CODE § 22575 (b)(5)).

51. Compliance with AB 370 seems to circumvent the purpose of DNT. An informal survey shows that most of the companies complying with AB 370 offer a vague statement saying that they ignore DNT. These notices are usually contained somewhere in the privacy policy or in a file linked to from the privacy policy.

wide adoption. First, there is no agreement among participants on the treatment of a DNT request by a website, i.e., as to how the website should respond.[52] Second, only a few prominent companies such as Mozilla, Twitter, and AP News have publicly encouraged DNT, and thus the list of implementers is quite modest.[53] Lastly, if there were a new standard that called for all companies to perform a minimum set of actions upon receipt of a DNT signal, companies might simply refuse to allow access to users requesting DNT.

3. Research on Automated Understanding of Privacy Policies

Researchers have also considered whether automated processing of privacy policies will be able to provide users with meaningful information for notice and choice.[54] One recent study explored the possibility of using automated processing and crowdsourcing to interpret website privacy policies.[55] The study relied on data provided by ToSDR.org, a crowdsourcing project that examined a limited set of privacy policies and that does not use a scientifically-based rating approach for those policies.[56] The study did, however, find inherent limitations due to "ambiguity of language" and variant human interpretations.[57]

Other studies further investigated the feasibility of leveraging natural language processing and machine learning techniques to tackle the problems of automatic categorization of privacy policies[58] and grouping segments of policies based on the privacy issues they address.[59] These studies shed light

52. The World Wide Web Consortium ("W3C") successfully published a late-stage draft of the technical mechanisms to send and receive DNT signals. *See Tracking Preference Expression (DNT) W3C Last Call Working Draft*, WORLD WIDE WEB CONSORTIUM (Apr. 24, 2014), http://www.w3.org/TR/tracking-dnt/.

53. Mozilla published an implementation guide with example source code. *See The Do Not Track Field Guide*, MOZILLA DEVELOPER NETWORK (Oct. 8, 2014), https://developer.mozilla.org/en-US/docs/Web/Security/Do_not_track_field_guide. But, there is no consensus on the treatment of the signal. Several companies have announced they honor DNT. *See Do Not Track: Implementations*, DONOTTRACK.US, http://donottrack.us/implementations/ (last visited May 19, 2015).

54. *See* Sadeh et al., *supra* note 2;_Bellovin & Zimmeck, *supra* note 2; Zimmeck & Privee, *supra* note 2.

55. Bellovin & Zimmeck, *supra* note 2; *Privee*, *supra* note 2.

56. *See supra* note 55.

57. *Id.*

58. Waleed Ammar et al., *Automatic Categorization of Privacy Policies: A Pilot Study*, CARNEGIE MELLON UNIV., SCH. OF COMPUTER SCIENCE, TECHNICAL REPORT NO. CMU-ISR-12-114, CMU-LTI-12-019, (2012).

59. Fei Liu et al., *A Step Towards Usable Privacy Policy: Automatic Alignment of Privacy Statements*, *in* PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON COMPUTATIONAL LINGUISTICS (COLING) (Aug. 2014); Rohan Ramanath et. al, *Unsupervised Alignment of Privacy*

on automatic methods of understanding privacy policies; however, it is not clear if the existing natural language techniques are able to fully decode the sophistication and ambiguity of privacy policies. A more promising approach will likely involve combining such techniques with machine learning and crowdsourcing, hence the importance of this study.

Another study examined the manual translation of privacy policies into a specialized mathematical logic.[60] The study results include heuristics for mapping variant interpretations into a single, canonical representation expressed in logic and a demonstration of how this logical representation can be used to answer questions about information collection, use, and sharing. For example, one heuristic includes mapping certain verbs, such as "transfer," "share," and "access" to events in which a data holder shares personal information with a third party.[61] In particular, the verb "access" is ambiguous because it can map to collection, use, or sharing depending on the stakeholder viewpoint, i.e., who has access. Other ambiguities, such as omissions, generic terms, and terms that have varying technical interpretations can lead to variant interpretations, some of which may be unintended by the policy authors. While the formalization does enable automated reasoning to detect policy conflicts due to ambiguous policy statements, it requires special training to perform the translation into logic. As with any policy document, the logical representation must also be maintained as the natural language policy changes. This prior work leaves open the question of how automated processing and crowdsourcing might function on an enormously broad set of privacy policies with a systematic approach to rating those policies. Although the preliminary results[62] are promising, it is not clear from this prior work whether a level of automation can be reached that would enable the process to be conducted on a web scale.

4. Unanswered Questions for Automated and Crowdsourced Understanding

In light of the present state of research, this study tests the comprehension and clarity of privacy notices on a larger scale, with the aim

Policies using Hidden Markov Models, *in* PROCEEDINGS OF THE ANN. MEETING OF THE ASSOC. FOR COMPUTATIONAL LINGUISTICS (ACL) (June 2014).

60. Travis Breaux et. al., *Eddy, A Formal Language for Specifying and Analyzing Data Flow Specifications for Conflicting Privacy Requirements*, 19 REQUIREMENTS ENG'G J. 281, 281–307 (Dec. 2013).

61. *Id.*

62. Travis Breaux & Florian Schaub, *Scaling Requirements Extraction to the Crowd: Experiments on Privacy Policies*, *in* 22ND IEEE INT'L REQUIREMENTS ENG'G CONFERENCE (2014), *available at* http://www.cs.cmu.edu/~breaux/publications/tdbreaux-re14.pdf.

of making a prognosis about the viability of large-scale semi-automated analysis and review of privacy policies. Prior work shows that policy ambiguity may challenge the ability of natural language processing to be effective. Crowdsourcing may not fully remedy these ambiguities, but crowdsourcing might help overcome some of these limitations depending on how far the interpretation of non-ambiguous elements might be scaled (e.g., does it always require expert annotators and could one leverage the so-called "wisdom of the crowds"?). Accordingly, this study is designed to explore the clarity of privacy policies in more detail by examining how three groups with different levels of expertise understand privacy notices. The goal is to elicit commonalities and differences in the comprehension and interpretation of websites' privacy policies across groups of participants with varying legal backgrounds and training.

III. METHODOLOGY

The research methodology was designed to discover how three different user groups would each interpret specific language in privacy policies. As discussed below, the participant groups were chosen to reflect expert, knowledgeable, and crowd workers representing typical users. Privacy policies were systematically collected from the web, and a survey was created to probe user understanding of the policies. In addition, background information was collected from the survey respondents.

A. THE PARTICIPANT GROUPS

Three groups participated in this study: 1) crowd workers representing typical users; 2) knowledgeable users; and 3) privacy policy experts. These groups were recruited as follows:

> 1) *Crowd workers* were recruited on Amazon Mechanical Turk ("MTurk") as a representative sample of the general population.[63] MTurk is an internet marketplace that uses human intelligence by crowdsourcing the performance of tasks requested by individuals or business.[64] The data used for this study came from twenty-eight crowd workers.[65] Previous studies have shown that MTurk provides a suitable participant pool for conducting research studies

63. MTurk is an Amazon website that pays users to complete proposed tasks.

64. *See* AMAZON MECHANICAL TURK (BETA), http://aws.amazon.com/mturk/ (last visited May 19, 2015).

65. As discussed in *infra* Sections III.B & C, five crowd workers annotated each of the six policies. Of the 28 crowd workers, 27 annotated only one of the six policies and 1 crowd worker annotated 3 of the six policies. The 1 crowd worker who annotated multiple policies annotated the Barnes & Noble, ABC News, and Washington Post policies.

and that the demographic distribution of crowd workers on MTurk is comparable to the general U.S. population.[66] These workers were paid $6.00 per reviewed policy. To be eligible to participate, these workers were required to have at least a 95% approval rating for 500 completed tasks on MTurk and be U.S. residents.[67] U.S. residency was verified with a question asking about the worker's country of residence. Multiple screening checks were applied in order to determine whether a crowd worker made an honest effort in completing the task. This vetting consisted of checking for the duration spent on the task, whether question responses were accompanied by meaningful text selections (see below), and whether the participant provided actual words for the answers to a Cloze test, a test that requires participants to replace several missing words in a piece of text to assess their general reading comprehension. All crowd worker submissions satisfied these checks, likely because the required qualification (95% approval rating on 500 tasks) and the relatively high pay ($6.00) were sufficient to motivate honest participation in the study.

2) *Knowledgeable users* consisted of five graduate students with a background in law, public policy, or computer science who were recruited from Fordham University, Carnegie Mellon University, and the University of Pittsburgh. These five knowledgeable users were hired as research assistants.

3) *Privacy policy experts* consisted of four of the study authors who are experienced law and public policy scholars. The purpose of these expert annotations was to determine the degree of agreement between experts, as well as to investigate the deviation of professional interpretation from the interpretation by knowledgeable users and crowd workers.

B. PRIVACY POLICY DATA SET

We collected unique privacy policies from the top websites ranked by Alexa.com, the most prominent measurement company for web traffic data.[68] These policies were collected during a period of six weeks between

66. *See* Tara S. Behrend et al., *The Viability of Crowdsourcing for Survey Research*, 43 BEHAVIOR RES. METHODS 800, 800–13 (2011); Gabriele Paolacci et al., *Running Experiments on Amazon Mechanical Turk*, 5 JUDGMENT & DECISION MAKING 411, 411–19 (2010); Gabriele Paolacci & Jesse Chandler, *Inside the Turk: Understanding Mechanical Turk as a Participant Pool*, 23 CURRENT DIRECTIONS IN PSYCHOL. SCI. 184, 184–88 (2014).

67. The MTurk rating level was set to assure that workers would take the task seriously and the U.S. residency requirement was set to assure that workers would not assume rights that exist in foreign countries.

68. Alexa ranks the popularity of websites based on their traffic. *See About Us*, ALEXA (2014), http://www.alexa.com/about/.

December 2013 and January 2014. They provide a snapshot of privacy policies from mainstream websites based on Alexa.com's website categories.[69] Since locating a website's policy is not a trivial task, we crowdsourced the privacy policy document collection using MTurk.[70]

In an earlier exploratory study, fifteen websites were selected from each of the Alexa.com "news" and "shopping" categories and were used for initial crowdsourcing analysis. The websites were selected in a top-down fashion using the rankings provided by Alexa.com. Additionally, two websites (amazon.com, yahoo.com) were set aside as a development data set and used for testing the crowdsourcing interface.

In this study, we focus on U.S commercial websites. From the policy data set, three privacy policies were manually selected from the "news" category and three policies were manually selected from the "shopping" category. The main websites for the companies whose privacy policies were selected for study are listed below along with the date of each policy's last revision as of the moment of collection:

News sites:

- ABC News (December 30, 2013): http://abcnews.go.com/
- Washington Post (November 15, 2011): http://www.washingtonpost.com/

69. Of the seventeen categories, two were excluded: the "Adult" and the "World" category. The "World" category was excluded since it contained mainly popular websites in different languages, and we opted to focus on policies in English in this study.

70. Though many well-regulated commercial websites provide a "privacy" link on their homepages, not all do. Neither is there a standardized URL format for privacy policies. Even once the policy's URL is identified, extracting the policy text presents the usual challenges associated with scraping documents from the web. Since every site is different in its placement of the document (e.g., buried deep within the website, distributed across several pages, or mingled together with Terms of Service) and format (e.g., HTML, PDF, etc.), and since we aimed to preserve as much document structure as possible (e.g., section labels), full automation was not a viable solution. For each website, we created a "human intelligence task" or HIT in which a worker was asked to copy and paste the following privacy policy-related information into text boxes: (i) privacy policy URL; (ii) last updated date (or effective date) of the current privacy policy; (iii) privacy policy full text; and (iv) the section subtitles in the top-most layer of the privacy policy. To identify the privacy policy URL, workers were encouraged to go to the website and search for the privacy link. Alternatively, they could form a search query using the website name and "privacy policy" (e.g., "Amazon.com privacy policy") and search in the returned results for the most appropriate privacy policy URL. Each HIT was completed by three workers who were each paid $0.05 per HIT. The collected privacy policies were further validated through manual review by one of the authors to ensure quality annotations.

- Weather Underground (October 30, 2013): http://www.wunderground.com/

Shopping sites:

- Barnes and Noble (May 7, 2013): http://www.barnesandnoble.com/
- Lowe's (April 25, 2013): http://www.lowes.com/
- Overstock (January 9, 2013): http://www.overstock.com/

These six privacy policies are included in Appendix A.

C. PRIVACY POLICY SURVEY AND ANNOTATIONS

The study focused on three key privacy policy elements: the collection of information, sharing of information, and deletion of information. These were chosen to reflect important user concerns and were selected based on an analysis of FTC privacy enforcement actions, which identified surreptitious collection, unauthorized disclosure, and wrongful retention of personal information as the most significantly contested online information practices.[71] The study asked about four information types shown to be highly relevant to users in previous studies.[72] These information types were: contact information (such as an address), financial information (such as payment information), current location information, and health information.

To discover commonalities and differences in interpretation between our different participant groups, we created a survey for participants that asked nine questions about different data practices described in a website's privacy

71. *See* JOEL R. REIDENBERG, ET AL., FORDHAM CTR. ON LAW & INFO. POL'Y, PRIVACY ENFORCEMENT ACTIONS (June 24, 2014), http://law.fordham.edu/assets/CLIP/CLIP_Privacy_Case_Report_-_FINAL.pdf [hereinafter PRIVACY ENFORCEMENT ACTIONS]. A fourth aspect—inadequate security for personal information—was not considered in this study, because privacy policies often contain only vague statements on security measurements.

72. *See* Mark S. Ackerman, Lorrie Faith Cranor & Joseph Reagle, *Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences*, *in* PROCEEDINGS OF THE 1ST ACM CONFERENCE ON ELECTRONIC COMMERCE (EC), 1–8 (1999); Adam N. Joinson, Ulf-Dietrich Reips, Tom Buchanan & Carina B. P. Schofield, *Privacy, Trust, and Self-Disclosure Online*, 25 HUMAN–COMPUTER INTERACTION 1 (2010); Craig E. Wills & Mihajlo Zeljkovic, *A Personalized Approach to Web Privacy: Awareness, Attitudes and Actions*, 19 INFO. MGMT. & COMP. SECURITY 53 (2011); Pedro G. Leon, et al., *What Matters to Users?: Factors That Affect Users' Willingness to Share Information With Online Advertisers*, *in* PROCEEDINGS OF ACM SYMPOSIUM ON USABLE SECURITY AND PRIVACY (SOUPS) 7 (2013).

policy. These questions (four collection questions, four sharing questions, one deletion question) are described below.

Each study participant was asked to answer the set of survey questions for each of the respective policies. For each answer, the participant was asked to select the text from the policy sections corresponding to the chosen answer. Each of the experts annotated the same set of six privacy policies specified above. While each of the knowledgeable users and crowd workers annotated more than six policies, these six policies reviewed by the experts were the only policies considered among those surveyed for the other participants.[73] The annotation process was completed using an online tool created for the task. Participants would select sentences and text passages in the policy with the mouse and then add those passages into a text field under the question by clicking a button. Participants could add one or multiple policy statements for their answers. All answer responses other than the *not applicable* response option required the selection of at least one accompanying text segment.[74]

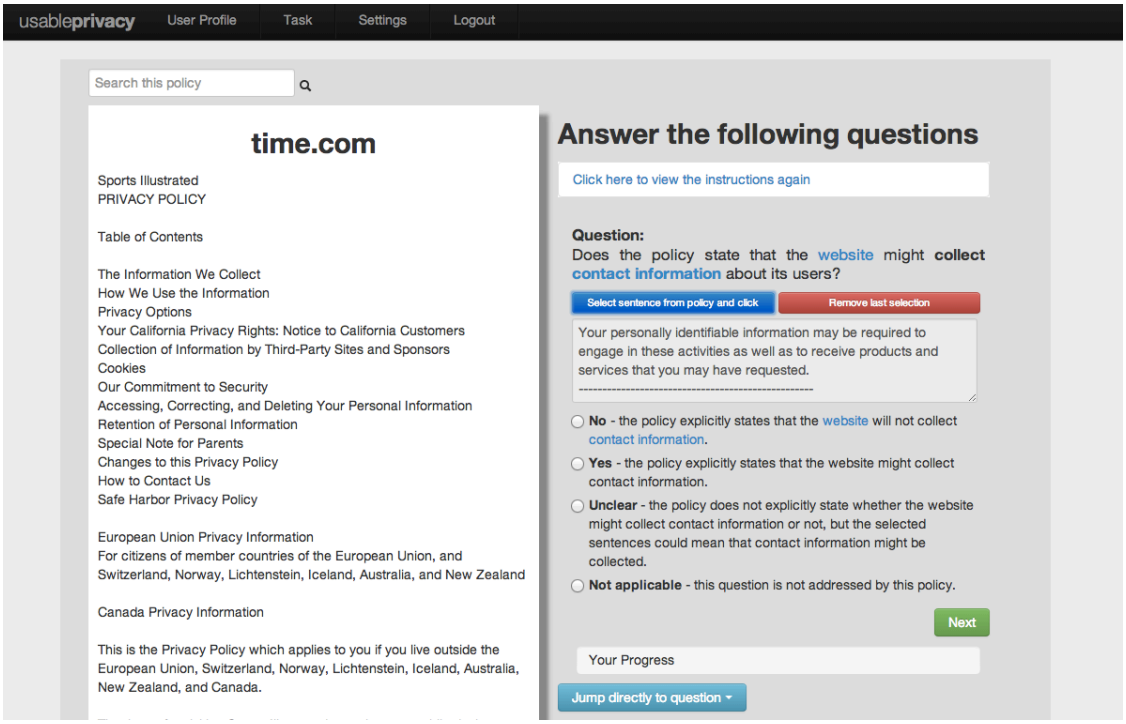
The annotation tool and the wording of questions and response options were refined over multiple iterations of pilot testing and an exploratory experiment. The pilot experiment used six participants (law and computer science graduate students) who each annotated fifteen policies and provided feedback in semi-structured interviews.

73. MTurk crowd workers could choose to annotate only one policy or multiple policies and were compensated separately for each. Crowdsourcing tasks were created so that we obtained at least five annotations from different crowd workers per policy. The majority of MTurk crowd workers chose to annotate only a single policy. Each knowledgeable user annotated twenty- privacy policies in total. We further conducted semi-structured interviews with all five knowledgeable users to gain deeper insights into their annotation strategies and their interpretation of our elicitation questions and policy statements.

74. The online annotation tool further provided participants with detailed instructions on how to complete the annotation task. Participants were instructed to answer questions only for the company's main website and ignore privacy policy statements pertaining to other aspects of a company's business, such as mobile applications, physical stores, or other websites operated by the same company. Participants were further asked to ignore statements pertaining to a specific subset of users, such as statements addressing California privacy laws, E.U. Safe Harbor regulation, or the Children's Online Privacy Protection Act. The instructions further clarified that the most fitting option should be selected based on the information given in the shown privacy policy and that "unclear" should be selected if multiple options would seem to apply, statements are ambiguous or contradictory, or if access to additional linked policies (e.g., a separate cookie policy) would likely be required to answer a question conclusively. We also provided definitions for common terms in the questions and response options (see blue highlights in Figure 1) for further clarification.

The final version of the online tool is illustrated in Figure 1 below. The scrollable privacy policy is displayed on the left side of the screen, and one question is shown at a time in a sidebar on the right. Participants could either progress through the questions sequentially or jump between questions in order to enable participants to quickly translate discovered policy statements into responses to our survey questions.

Figure 1
Online tool for privacy policy annotations.



display a tooltip with a definition of the respective term.

The survey questions on collection of personal information (Q1–Q4) inquired whether contact information (Q1), financial information (Q2), current location information (Q3), or health information (Q4) is being collected by the given website. Participants could choose between four answer options:

> **Answer Option 1: No**—the policy explicitly states that the website will not collect [specified type of information (i.e., contact, financial, etc.)].
>
> **Answer Option 2: Yes**—the policy explicitly states that the website might collect [specified type of information (i.e., contact, financial, etc.)].

> **Answer Option 3: Unclear**—the policy does not explicitly state whether the website might collect [specified type of information (i.e., contact, financial, etc.)] or not, but the selected sentences could mean that [specified type of information (i.e., contact, financial, etc.)] might be collected.
>
> **Answer Option 4: Not applicable**—this question is not addressed by this policy.

While the *Yes* and *No* options capture explicit statements in the policy, the *Unclear* option enabled participants to note ambiguity in the policy regarding the collection of a specific information type. The *Not applicable* option, on the other hand, allowed for distinguishing between a policy containing ambiguous statements or no statement at all.

The questions on sharing of personal information (Q5–Q8) inquired whether a website would share contact information (Q5), financial information (Q6), current location information (Q7), or health information (Q8) with third parties. If the policy stated that personal information would be shared with third parties, participants could indicate whether the information would be shared for the purpose of fulfilling a core service (e.g., payment processing or delivery of purchased goods), for purposes other than core services, or for purposes other than core services but only with explicit consent. Hence, the sharing of personal information questions offered six response options:

> **Answer Option 1: No sharing**—the policy explicitly states that the website will not share [specified type of information (i.e., contact, financial, etc.)] with third parties.
>
> **Answer Option 2: Sharing for core service only**—the policy explicitly states that the website might share [specified type of information (i.e., contact, financial, etc.)] with third parties, but only for the purpose of providing a core service, either with explicit or implied consent/permission from the user.
>
> **Answer Option 3: Sharing for other purpose**—the policy explicitly states that the website might share [specified type of information (i.e., contact, financial, etc.)] with third parties for other purposes. The policy makes no statement about the user's consent/permission or user consent is implied.
>
> **Answer Option 4: Sharing for other purpose (explicit consent)**—the policy explicitly states that the website might share [specified type of information (i.e., contact, financial, etc.)] with third parties for a purpose that is not a core service, but only if the user provided explicit permission/consent to do so.

> **Answer Option 5: Unclear**—the policy does not explicitly state whether the website might share [specified type of information (i.e., contact, financial, etc.)] with third parties or not, but the selected sentences could mean that *contact information* might be shared with third parties.
>
> **Answer Option 6: Not applicable**—this question is not addressed by this policy.

The question on deletion of personal information (Q9) asked about the website's respective deletion policy statements. We explicitly excluded any statements concerning retention for legal purposes, as we sought to assess policy statements that relate to issues of wrongful retention of personal information.[75] If the policy explicitly stated that information could be removed, participants could indicate whether information would be removed fully or whether some or all of the information may be retained for other purposes:

> **Answer Option 1: No removal**—the policy explicitly states that the user will not be allowed to delete their personal data.
>
> **Answer Option 2: Full removal**—the policy explicitly states that users may delete their personal data and that no data will be retained for any purpose, whether the data was provided directly by the user, generated by the user's activities on the website, or acquired from third parties.
>
> **Answer Option 3: Partial removal**—the policy explicitly states that users may delete their personal data but some/all of the data might be retained for other purposes, whether the data was provided directly by the user, generated by the user's activities on the website or acquired from third parties.
>
> **Answer Option 4: Unclear**—the policy does not explicitly state whether users may delete their personal data or not (e.g., it only talks about editing information).
>
> **Answer Option 5: Not addressed**—this question is not addressed by this policy.

After answering all nine annotation questions for a given privacy policy, participants were shown an additional screen with three questions asking them whether they had ignored parts of the privacy policy because they did not refer to the company's main website (yes/no), whether the privacy policy contained pointers or links to other policy documents

75. *See* PRIVACY ENFORCEMENT ACTIONS, *supra* note 71.

(yes/no), and to rate "how easy or difficult it was to answer the previous nine questions for this privacy policy" on a five-point Likert scale (from "very difficult" to "very easy").

D. BACKGROUND DEMOGRAPHICS

Additionally, after completing the privacy policy annotations, participants were further asked to complete a background questionnaire, which consisted of multiple parts. First, participants were asked to rate their ability to understand legal texts on a five-point scale (from "very difficult" to "very easy"). This self-assessment was followed by questions about the level of legal training they had received and whether they worked in a position that required legal expertise. The second part collected basic demographic information, namely, gender, education level, and primary occupation. In the third part, participants were presented with a Cloze test—a test that requires participants to replace several missing words in a piece of text—to assess their general reading comprehension.[76] The background questionnaire closed with a number of questions about the annotation experience. Participants were asked to rate the perceived ease or difficulty of answering each of the nine annotation questions on a seven-point scale (from "very difficult" to "very easy") and the helpfulness of provided instructions and definitions on a seven-point scale (from "not at all helpful" to "very helpful"). Lastly, an open-ended question allowed participants to further comment on difficulties with terms, questions, or answer options.

In terms of gender and age, the twenty-eight crowd workers who annotated the six relevant privacy policies were 64% male (18) and 36% female (10). They ranged in age from 22 to 63 (with a median age of 29). Our group of five knowledgeable users was 40% male (2) and 60% female (3). Their ages were slightly younger (23 to 35 years of age with a median age of 24). The four privacy policy experts were 75% male (3) and 25% female (1). They were slightly older in comparison (34 to 53 years with a median age of 42).

With respect to education, all four experts have a graduate degree, and all five knowledgeable users have at least a bachelors degree (one has a graduate degree). The crowd workers were less educated, with only 46% having a bachelors degree or higher 2.

76. *See* CAMBRIDGE ENGLISH PROFICIENCY CERTIFICATE OF PROFICIENCY IN ENGLISH CEFR LEVEL C2, HANDBOOK FOR TEACHERS, UNIV. OF CAMBRIDGE 14 (2013), *available at* https://www.teachers.cambridgeesol.org/ts/digitalAssets/117848_Cambridge_English_Proficiency__CPE__Handbook_2013.pdf.

Crowd workers' primary occupations were diverse and included administrative support (6), service industry (4), unemployed (4), art/writing/journalism (3), business/management/financial (3) student (2), art/writing/journalism (3), business/management/financial (3), education (2), and other (4). None of the crowd workers selected "legal (e.g., lawyer, law clerk)" as a primary occupation. Eighteen crowd workers indicated they had no legal training at all. Seven indicated that they had no legal training but that their background in another field provided them with some legal experience. Finally, three indicated that they were knowledgeable in legal matters but had no formal training. Privacy policy experts were all researchers and scholars, and two of them studied law. Knowledgeable users were all current students of law, computer science, or public policy.

IV. DATA COMPARISONS

This part reports on the data collected as a result of the methodology described above. The part will first analyze the empirical data on intra-group annotator agreement. Then it will analyze the empirical data on inter-group annotator agreement. As will be shown, high levels of agreement within a group ('intra-group" agreement) does not guarantee that this group converged on the same answers as other groups ("inter-group" agreement). The part will conclude with a discussion of qualitative trends observed in the data.

A. INTRA-GROUP ANNOTATOR AGREEMENT

The degree of agreement within each user group is shown in Tables 1–3.[77] Table 1 shows intra-group agreement for all questions and over the six policies annotated by the experts group for data collection, while Tables 2 and 3 show intra-group agreement for data sharing and deletion respectively. Intra-group agreement is measured by the median level of group member agreement on the same answer across all the policies.[78] First, the most frequently chosen answer (mode) for each question in each policy was identified. Then, to determine the level of agreement with the mode answer, the percentage of annotators selecting that mode answer was calculated for

77. The tables do not distinguish between the website policies of news and shopping sites. The agreement rate among annotators was almost identical between the news and shopping categories for knowledgeable users. Crowd workers had similar agreement rates to the knowledgeable users on news sites, but slightly less agreement on the policies for shopping sites.

78. Because of the small number of annotators, mean and standard deviation calculations would not provide an accurate representation of group member consensus.

each question in each policy. The median level of agreement across all policies for the same question was calculated to reflect the group consensus on an answer choice. A median value of 100% means that all group members agree on the same answer choice for the survey question for at least four out of the six policies and share the same understanding of those privacy policies. As the median agreement declines, the group members understand some of the policies differently from each other. Any value less than 100% reflects that the annotator group had no consensus answer on the same question for three or more policies—the lower the value, the greater the disagreement. The tables also reflect the median level of agreement when related answer choices were combined.[79] By combining answer choices, we can determine if there is at least a consensus on the way the policy broadly treats information. When answer choices are combined, the table shows the median level of agreement for each answer combination. Differences in the mode answer choice across the policies are reflected by median calculation based on those policies with the same mode.[80] The difference between the median level of agreement across all answer choices and the median agreement when several answer choices are combined reflects that group members recognize that the policy addresses a particular point, but they do not share the same understanding of the nuances.

Complete agreement by all members within each of the groups was uncommon and, as shown in the tables, agreement was not distributed evenly across questions. For data collection as reflected in Table 1 below, experts had a consensus on contact and location information (100% median level of agreement across all policies), but they varied in their understanding of the collection of financial and health information (87.5% and 50% respectively). Knowledgeable users shared the same understanding on the collection of contact and financial information (100% median level of agreement across all policies), but not location (70%) or health information (80%). Interestingly, the knowledgeable users had greater agreement on health information than

79. In Table 1, we combined the answer options "Unclear" and "Not applicable" as they were not differentiated consistently by all annotators. In Table 2, we combined answer choices 2–4 ("Sharing for core service only," "Sharing for other purpose," and "Sharing for other purpose (explicit consent)"), as all three of them describe that sharing with third parties is taking place, but differentiate between consent models; we further combined answer choice 5–6 ("Unclear" and "Not applicable") for the same reasons as above. In Table 3, we combined answer choices 2–3 ("full removal" and "partial removal") as they describe that removal is possible but vary in whether data is retained; as well as answer choices 4–5 ("Unclear" and "Not applicable") for the same reasons as above. *See infra* Tables 1–3.

80. This means the median score for a given answer choice combination may be based on fewer than six policies and is independent from the median calculations of the other answer choice combinations.

the experts. These results likely indicate that knowledgeable users missed important ambiguity in the privacy policy. Lastly, crowd workers had the lowest level of shared understanding compared to the other groups for contact information (90%), location information (90%), financial information (50%), and health information (70%). The crowd workers had a higher level of agreement on location information than the knowledgeable users, though less than the experts.

Table 1

Data Collection: Intra-group Agreement

Level of Agreement on the Same Answer (Median Across All Policies)	**Collect Contact**	**Collect Financial**	**Collect Location**	**Collect Health**
Experts				
All choices	100 %	87.5 %	100 %	50 %
Answer Choice 1	n/a	n/a	n/a	n/a
Answer Choice 2	100 %	100 %	100 %	n/a
Answer Choice 3-4	n/a	75 %	n/a	100 %
Knowledgeable Users				
Using All Answers	100 %	100 %	70 %	80 %
Answer Choice 1	n/a	n/a	n/a	n/a
Answer Choice 2	100 %	100 %	90 %	n/a
Answer Choice 3-4	n/a	90 %	100 %	100 %
Crowd Workers				
Using All Answers	90 %	50 %	90 %	70 %
Answer Choice 1	n/a	n/a	n/a	n/a
Answer Choice 2	90 %	100 %	90 %	n/a
Answer Choice 3-4	n/a	60 %	n/a	100 %

For data sharing, Table 2 (shown below) indicates that the experts did not have a high level of consensus on the meaning of the privacy policies (ranging from 75% median level of agreement on contact information across all policies to 50% on health data). However, the level of agreement

improves when the disclosure choices are aggregated (i.e., when answer choices 2–4 are collapsed into one). This means that the experts recognize, though never unanimously, that sharing occurs, but they disagree as to the conditions for sharing as set out in the privacy policies. The knowledgeable users had weak agreement on their interpretations of sharing for contact information (60% median level of agreement across all policies), financial information (50%), and location information (60%). Oddly, the knowledgeable users' level of agreement for health information across all policies was greater than that for the experts (80% median level vs. 50% median level). This means that the knowledgeable users did not perceive as much ambiguity as the experts and suggests that the knowledgeable users may have misunderstood the privacy policies' sharing terms for health information. The crowd workers similarly had weak agreement on their interpretation of policy statements on sharing and, similarly, had a greater consensus on the sharing of health information as compared to the experts.

Table 2

Data Sharing: Intra-group Agreement

Level of Agreement on the Same Answer (Median Across All Policies)	**Share Contact**	**Share Financial**	**Share Location**	**Share Health**
Experts				
All Choices	75 %	62 .5 %	62 .5 %	50 %
Answer Choice 1	n/a	n/a	n/a	n/a
Answer Choice 2–4	87 .5 %	87 .5 %	75 %	n/a
Answer Choice 5–6	n/a	n/a	75 %	75 %
Knowledgeable Users				
All Choices	60 %	50 %	60 %	80 %
Answer Choice 1				
Answer Choice 2–4	80 %	80 %	100 %	n/a
Answer Choice 5–6	60 %	60 %	100 %	100 %
Crowd Workers				
All Choices	60 %	60 %	40 %	80 %
Answer Choice 1	n/a	n/a	n/a	n/a
Answer Choice 2–4	100 %	60 %	60 %	n/a
Answer Choice 5–6	n/a	100 %	70 %	100 %

For deletion, Table 3 below shows that the experts were not in complete agreement on the specific terms for data deletion (75% median level of agreement across all policies). They did, however, agree (100%) on whether some deletion options were available when the full and partial deletion options were aggregated. Knowledgeable users had less agreement than the experts on the terms of deletion policies (60%), but like the experts, when full and partial deletion choices were combined, the knowledgeable users had a complete consensus that at least some deletion was possible (100%). Crowd workers had the least agreement on data deletion (50%), but also reached complete consensus on policies that allowed at least partial deletion (100%).

Table 3

Data Deletion: Intra-group Agreement

	Level of Agreement on the Same Answer (Median Across All Policies)
Experts	
All Choices	75 %
Answer Choice 1	n/a
Answer Choice 2-3	100 %
Answer Choice 4-5	n/a
Knowledgeable Users	
Using All Answers	60 %
Answer Choice 1	n/a
Answer Choice 2-3	100 %
Answer Choice 4-5	n/a
Crowd Workers	
Using All Answers	50 %
Answer Choice 1	n/a
Answer Choice 2-3	100 %
Answer Choice 4-5	n/a

The lack of complete agreement within each group was further confirmed by the Fleiss' Kappa (*K*) statistic. The Fleiss' Kappa statistic is used to compute the proportion of agreement above chance for multiple

raters who independently rate the same number of items.[81] Inter-rater reliability statistics that account for chance agreement factor in the probability distribution that answer choices are selected across the rating sample. If there is a high probability that an answer choice will be chosen across items, then there is a higher probability that raters will select this option by chance alone. Landis and Koch proposed arbitrary divisions for Kappa that rank 0.41–0.60 as moderate agreement and 0.61–0.80 as substantial agreement.[82] The computed Fleiss' Kappa for each group of raters are as follows: Expert $K = 0.496$, Knowledgeable Users $K = 0.703$, and Crowd Workers $K = 0.500$.

B. INTER-GROUP ANNOTATOR AGREEMENT

The shared understandings across user groups are shown in Tables 4–6. Table 4 shows the inter-group agreement levels for data collection. Table 5 reflects the level of inter-group agreement on data sharing. Table 6 presents the interpretation of data deletion. The tables were calculated using combined answer choices to determine whether there were shared understandings of the broad practices.[83] Inter-group agreement was measured across all the policies by comparing the answer choices of the knowledgeable users and crowd workers with the mode answer choices of the experts.[84]

81. *See* Joseph Fleiss, *Measuring Nominal Scale Agreement Among Many Raters*, 76 PSYCHOL. BULL. 378 (1971).

82. *See* J. Richard Landis & Gary G. Koch, *The Measurement of Observer Agreement for Categorical Data*, 33 BIOMETRICS 159 (1977).

83. In Table 4, we combined the answer options "Unclear" and "Not applicable" as they were not differentiated consistently by all annotators. In Table 5, we combined answer choices 2–4 ("Sharing for core service only," "Sharing for other purpose," and "Sharing for other purpose (explicit consent)") as all three of them describe that sharing with third parties is taking place, but differentiate between consent models; we further combined answer choice 5-6 ("Unclear" and "Not applicable") for the same reasons as above. In Table 6, we combined answer choices 2–3 ("full removal" and "partial removal") as they describe that removal is possible but vary in whether data is retained; as well as answer choices 4–5 ("Unclear" and "Not applicable") for the same reasons as above. *See infra* Tables 4, 6.

84. One caveat to the analysis is that the consensus category is defined as the median level of agreement. For statisticians, determining the level of agreement based on consensus category has two potential drawbacks. First, consensus can be based on the mode, median, or mean agreement level, which makes it difficult to compare results across studies that use a different basis for consensus. Second, there are different response patterns that can lead to the same consensus level and same conclusion, despite different variability in the responses (i.e., the consensus technique is not sensitive to variability). Another way to examine consensus comes from Vanbelle and Albert who describe a novel agreement index that is a natural extension of Cohen's Kappa for measuring the overall proportion of agreement above chance between two groups of raters that also accounts for the heterogeneity of each group. *See* S. Vanbelle & A. Albert, *Agreement Between Two Groups of Raters*, 74 PSYCHOMETRIKA 477 (2009). The Vanbelle/Albert Kappa for collection, sharing and

First, to establish the control values, the experts' most frequently chosen answer on each question for each policy was identified. The level of agreement among the experts selecting that mode answer was then calculated, and the median level of agreement across all six policies became the control value for the comparisons. A value of 100% means that all experts agreed on the same answer choice on the survey question for at least four of the six policies. As the value declines, the level of disagreement on the correct answer choice increases. For the knowledgeable users and crowd workers, the level of agreement with the experts' mode answer was calculated for each question and for each policy. The median levels of agreement for the knowledgeable users and crowd workers on the experts' mode answer across all six policies shows the alignment between these respective groups and the experts. For the knowledgeable users and crowd workers, a value of 100% on a particular question means that all group members agreed on the experts' mode answer choice and shared the same understanding of the privacy policy as the experts for at least four of the six policies.[85] As the value declines, the group members understand the policies differently from the experts.

For data collection, Table 4 below shows that the three groups shared the same understanding of the collection of health information (100% agreement with experts' answers). With respect to contact information, the knowledgeable users matched the experts (100%), but the crowd workers lagged in their comprehension (90%). The intra-group disagreements on health information reflect that ambiguities in the policies are being interpreted in the same way. The knowledgeable users had a consensus on financial information that matched the experts' most frequently chosen answer choice (100%). Since the experts were not unanimous on the answer choices with respect to financial information, the knowledgeable users may

deletion between groups is as follows: Expert-Knowledgeable K = 0.736, Expert-Crowd K = 0.581, and Knowledgeable-Crowd K = 0.555 for collection practices; Expert-Knowledgeable K = 0.485, Expert-Crowd K = 0.465, and Knowledgeable-Crowd K = 0.452 for sharing practices; and for all pairwise groups, K = 0.000 for deletion. The between-group Kappa shows higher levels of agreement above chance for experts and knowledgeable users for collection practices and no distinct differences between groups for sharing practices. For deletion, all raters agreed by assigning the same category to all items which raises the chance probability of assigning the category to 1.000. Consequently, there is no above chance agreement for this category of items.

85. Agreement between knowledgeable users and crowd workers does not necessarily mean the agreed-upon answer is objectively correct. To find out whether these two groups were likely to choose correct answers, we compared their answers to the answers given by the experts on the same policies.

not have been cognizant of the ambiguities seen by the experts. The crowd workers, however, were far off from the experts (40% median level of agreement with the experts' mode answer choice across all policies). This indicates that typical users have a much more difficult time understanding the collection of financial information. Lastly, the knowledgeable users had a significantly different interpretation of the collection of location information than the experts (70% median level of agreement with the experts' mode answer choice across all policies). The crowd workers were, however, in closer agreement with the expert answer choices (90%).

Table 4

Data Collection: Inter-group Agreement

	Collect Contact	**Collect Financial**	**Collect Location**	**Collect Health**
Experts Selecting Mode Answer Choice (Median Across All Policies)	100 %	87 .5 %	100 %	100 %
Knowledgeable Users Selecting Experts' Mode Answer Choice (Median Across All Policies)	100 %	100 %	70 %	100 %
Crowd Workers Selecting Experts' Mode Answer Choice (Median Across All Policies)	90 %	40 %	90 %	100 %

For data sharing, Table 5 below demonstrates that the experts had no complete agreement on answer choices for any of the types of data. However, with respect to contact information, the crowd workers agreed with the most frequently chosen expert answer (100% median level of agreement with experts), while the knowledgeable users lagged in their understanding (80%). This may indicate that the knowledgeable users reflected the difficulties that the experts had with policy ambiguity. For financial information, the knowledgeable users had only a modest level of agreement with the experts (50% median level of agreement), while the crowd workers were even more divergent (40%). For location information, the experts' agreement on an answer choice was modest (75% median level of agreement on the mode). Both the knowledgeable users and the crowd workers had a significantly different understanding (60% median level of agreement with experts' mode answer choice). Lastly, for health information, the knowledgeable users and crowd workers converged on the most

frequently chosen expert answer (100% median level of agreement). However, since the experts were divided on the answer choice, this finding suggests that the other groups may have missed nuances in the privacy policies with respect to potential sharing of health information.

Table 5

Data Sharing: Inter-group Agreement

	Sharing Contact	**Sharing Financial**	**Sharing Location**	**Sharing Health**
Experts Selecting Mode Answer Choice (Median Across All Policies)	87 .5 %	87 .5 %	75 %	75 %
Knowledgeable Users Selecting Experts' Mode Answer Choice (Median Across All Policies)	80 %	50 %	60 %	100 %
Crowd Workers Selecting Experts' Mode Answer (Median Across All Policies)	100 %	40 %	60 %	100 %

For data deletion, Table 6 illustrates that all groups agreed on the understanding of the privacy policies' language (100% median level of agreement). However, since the answer choices with respect to full and partial deletion were collapsed into one, this level of agreement may only reflect that all groups had the same understanding of the existence of, but not the conditions for, data deletion. The intra-group deviation on data deletion means that the policies have important ambiguity on the terms for data deletion, namely whether the policy covers full or partial deletion.

Table 6

Data Deletion: Inter-group Agreement

Experts Selecting Mode Answer Choice (Median Across All Policies)	100 %
Knowledgeable Users Selecting Experts' Mode Answer Choice (Median Across All Policies)	100 %
Crowd Workers Selecting Experts' Mode Answer (Median Across All Policies)	100 %

C. QUALITATIVE DATA ANALYSIS

1. Difficulty for Survey Respondents

For each policy, after annotators completed the nine survey questions, they were asked to rate on a 5-point Likert scale the difficulty of annotating that policy, where 1 was "very difficult" and 5 was "very easy." Averaged over the six policies, knowledgeable users rated the policies as easier to annotate on average (3.23) than the crowd workers (2.53). Interestingly, the experts also found the policies more difficult to annotate (2.88) than the knowledgeable users. Participants' self-reported ratings concerning their understanding of legal texts varied. The knowledgeable users rated their ability to understand legal texts higher on average (3.8) than the untrained crowd workers (2.29) or the experts (3.5). Looking at the average number of correct answers achieved in the general reading comprehension Cloze test, the experts and knowledgeable users performed on a similar level. Both groups exhibit a median score of seven correct answers (out of eight), with slight variations in the distributions (experts: mean = 6.75, std. dev. = 1.09; knowledgeable users: mean = 6.6, std. dev. = 0.49). The crowd workers exhibit lower reading comprehension with a median score of five correct answers (mean = 4.89, std. dev. = 2.02).

These results suggest that crowd workers may be hampered by less-developed reading comprehension skills in general and, more specifically, for legal text as indicated by their self-assessments. This lower reading comprehension matches the higher perceived difficulty of answering the annotation questions. Because the knowledgeable users and experts exhibit similar general reading comprehension skills, and assuming that experts have more experience in interpreting policy and legal text, the knowledgeable users may have either overestimated their abilities or the experts may have been more cautious in their self-assessment and difficulty ratings.

Table 7 below further shows the individual average difficulty ratings of the different groups for each of the six policies. One set of privacy policies (Lowe's, ABC News, and Washington Post) were perceived as considerably more difficult to annotate by the untrained crowd workers as compared to the other two groups. The Barnes and Noble policy was perceived as difficult to annotate by all three groups. For the Overstock and Weather Underground policies, the difficulty ratings of the experts and untrained crowd workers are quite similar, whereas the knowledgeable users rated them as easier in both cases. Also note that none of the average values reach the "easy" level (4.0).

Table 7

Average difficulty rating of answering the annotation questions for the given policies.

Policy	Experts (avg. ease)	Knowledgeable users (avg. ease)	Crowd workers (avg. ease)
Overstock	3.00	3.40	3.00
Lowe's	3.00	3.00	1.80
Barnes and Noble	2.25	2.60	2.40
ABC News	3.50	3.60	3.00
Weather Underground	2.50	3.20	2.80
Washington Post	3.00	3.60	2.20

2. Trends in Selected Text[86]

a) Consensus on Text Selection

In some instances, the experts achieved either exact or near-exact agreement on the language selected as well as the answer option. These instances of agreement are promising, as they suggest that some scenarios might be used to train natural language processing ("NLP") techniques and thus might be able to provide reliable interpretations of privacy policies. In particular, these instances suggest that crowdsourcing tools might be developed where only (or mostly) relevant text is shown to crowd workers, rather than tools where a crowd worker is required to read an entire policy to answer a particular question.[87] Where the experts achieved exact agreement,

86. This Section presents trends based on text selected by the experts and the knowledgeable users.

87. *See* Rohan Ramanath et al., *Identifying Relevant Text Fragments to Help Crowdsource Privacy Policy Annotations*, *in* PROCEEDINGS OF THE ASS'N FOR THE ADVANCEMENT OF ARTIFICIAL INTELLIGENCE CONFERENCE ON HUMAN COMPUTATION & CROWDSOURCING (2014).

they selected the same words or phrases and the same answer option.[88] Where the experts achieved near-exact agreement, it was typically the case that one annotator selected extra, immaterial words that another did not select, even though the experts selected the same answer option.[89]

Likewise, knowledgeable users were able to achieve exact or near-exact agreement on the language selections as well as the answer option.[90] As was apparent among experts, it was also typical for one or more knowledgeable users to select additional, immaterial words that others may have not selected, despite the fact that all annotators chose the same answer option.[91] Notably, there were also instances in which annotators would select the same text in support of different answers. This conflict was evident between both expert annotator groups and knowledgeable annotator groups. Ultimately, these occurrences testify to the difficulty of gathering uniform interpretations of privacy policy language, and present a potential challenge to the development of an NLP model that can provide reliable interpretations of privacy policies.[92] At the same time, these issues suggest that it might also be

88. *See, e.g.*, barnesandnoble.com Privacy Policy *infra* Appendix II. (Appendices for this Article are available at http://btlj.org/wp-content/uploads/2015/05/privacy-policies-appendix.pdf. An archived copy is available at https://archive.org/download/privacy-policies-appendix/privacy-policies-appendix.pdf.) All annotators selected the following: "we may collect personal information from you, for example your name, e-mail address, billing address, shipping address, phone number . . . ." Annotators' Responses to Survey Question 1 (on file with author).

89. *See, e.g.*, abcnews.go.com Privacy Policy *infra* Appendix I. For Survey Question 7, the annotators selected from the following range of text: "When you allow us to share your personal information with another company, such as: Electing to share your personal information with carefully selected companies so that they can send you offers and promotions about their products and services." Two annotators selected the darkly shaded language, where only one selected the more lightly shaded language as well. Responses to Survey Question 7 (on file with author).

90. *See, e.g.*, washingtonpost.com Privacy Policy *infra* Appendix V. As commonly seen, sentence selection was identical among all five knowledgeable users. To support their answers, every annotator selected the exact same text, which stated that "Washingtonpost.com asks for information such as your name, e-mail address, year of birth, gender, Zip code, country, street address." Responses to Survey Question 1 (on file with author).

91. *See, e.g.*, lowes.com Privacy Policy *infra* Appendix III. All knowledgeable users selected the following range of text: "You may choose to provide us with personal information (such as name, contact details and payment information), such as: Contact information, such as your name, address, telephone number, and email address, and your title or occupation." Responses to Survey Question 1 (on file with author).

92. Both expert and knowledgeable users tended to select the same text to support different answers when asked if a website permitted users to delete personal data. For example, all the experts in response to Survey Question 9 for the washingtonpost.com privacy policy, selected the statement that "[i]f you do not wish to receive the foregoing and therefore unregister from the site, please contact Customer Care and ask to have your

possible to build interfaces that boost the productivity of crowd workers by selectively displaying text fragments that are mostly relevant to the particular questions they are requested to annotate.

b) Interpretation of Policy Silence

Experts differed from knowledgeable users with respect to interpretation of policy silence. Generally, where a policy was silent on a particular practice, experts interpreted such silence to mean that the policy permitted the practice. This is the legal interpretation. Knowledgeable users, on the other hand, often misinterpreted silence to mean that the policy was unclear regarding the practice. Examples of this interpretive difference in the context of data collection, data sharing, and data deletion are described below.

i) Data Collection

One of the best examples of the interpretive difference in the data collection context can be found in Survey Question 2 ("Does the policy state that the website might collect financial information?") of the wunderground.com policy, which contains no explicit mention of "financial information."[93] In responding to that question, three out of four experts selected sentences that they interpreted to permit the website to collect financial information;[94] only one expert believed that the policy was unclear

registration account deleted." While one expert annotator believed that this statement indicated that users could partially remove their data, the remaining three experts selected this statement in support of the answer that it was unclear whether or not users could delete personal data.

With regard to deletion questions, even more frequently than experts, knowledgeable users tended to select the same sentences to support different answers. When responding to Survey Question 9, for example, all annotators for the www.abcnews.go.com privacy policy selected the same sentences which stated that "[y]ou may correct, update and delete your registration account" and "[y]ou may request access to the personal information we hold about you and that we amend or delete it and we request third parties with whom we have shared the information do the same." Though they all selected the identical text, two annotators believed that these statements indicated "full removal" of personal data, while two other annotators believed that they indicated "partial removal," and the remaining annotator believed that they indicated that it was "unclear" if users could or could not delete their data. Responses to Survey Question 9 (on file with author).

93. *See* wunderground.com Privacy Policy *infra* Appendix VI.

94. *See* wunderground.com (experts) Survey Question 2 (on file with author). Some relevant textual selections chosen by the three experts who said the policy collected financial information are:

> "We use information collected on the Services . . . to help fulfill your requests or in connection with the operation of the Services, for example

on the practice. However, knowledgeable users provided almost exactly opposite responses: one knowledgeable user selected sentences that led him or her to think the website could collect financial information,[95] while three knowledgeable users selected "unclear" and one selected "not applicable."

ii) Data Sharing

One of the best illustrations of the interpretive difference in the context of data sharing can be found in Question 7 ("Does the policy state that the website might share location information?") of the Barnes and Noble policy. The policy contains no explicit mention of sharing location information.[96] In responding to that question, three out of four experts selected sentences that they interpreted to permit the website to share location information;[97] only

> to . . . display information and advertisements that we believe match your interests and profile . . . ."
>
> "When your information is collected on the Services, it may be collected directly by or shared with a selected third parties in connection with the operation of the Services or the provision of services to you ("Third Party Processors"). These Third Party Processors may include, for example, companies that operate our online WunderStore, that process credit card information or handle shipping for Weather Underground . . . ."
>
> *See* wunderground.com Privacy Policy *infra* Appendix VI.

95. *See* wunderground.com (knowledgeable users) Survey Question 2. The one annotator selected the following text: "These Third Party Processors may include, for example, companies that operate our online WunderStore, that process credit card information or handle shipping for Weather Underground, that deliver materials to you via e-mail or postal service, that organize, administer, process, or provide advertising services, and/ or that analyze data on our behalf to help us provide more relevant offers to you and to eliminate the delivery of duplicate offers as well as correcting and/or updating users' data based on information we provide them."
See wunderground.com Privacy Policy *infra* Appendix VI.

96. *See* barnesandnoble.com Privacy Policy *infra* Appendix II.

97. *See* barnesandnoble.com (experts) Survey Question 7 (on file with author). Two annotators selected Answer Option 3 (Sharing for other purpose) and one chose Answer Option 4 (sharing for other purpose with explicit consent). Some relevant textual selections are:

> "These or related applications may also allow you to provide information directly to social networking sites including information about your purchases, physical location."
>
> "Like many online retailers, we and/or our third party providers use cookies to recognize you as you use or return to the Barnes & Noble Websites."
>
> "In addition, to provide location-based services on Devices or through Apps, Barnes & Noble and third party application providers may automatically collect real-time geographic location information or other location-based information about you."

one expert believed that the policy was unclear on the practice. On the other hand, no knowledgeable annotator selected sentences that led them to believe that the website may share users' location information. Instead, two annotators thought the policy was "unclear" on this matter,[98] and three selected "not applicable" to reflect the belief that the policy did not appear to address the question.

iii) Data Deletion

There were fewer interpretive differences in the context of data deletion. The annotators frequently agreed on whether a website permitted users to delete personal data.[99] However, annotators often indicated uncertainty in their responses. They would sometimes respond that it was "unclear" if a website allowed users to delete their information. Other times, annotators answered "partial removal" because it was not clear whether or not websites would retain some of users' data after deletion.[100] These issues arose because some policies addressed editing and correction, but did not explicitly discuss deletion, while other policies stated that users could request deletion, but did not guarantee that the website would actually delete information.

This general doubt among users likely reflects a lack of clarity within the privacy policies themselves. Many policies did not even acknowledge whether users would or would not be able to delete their personal data. For example,

> "[Y]our data may be transferred to or shared with a third party as part of a sale, merger, or acquisition of Barnes & Noble or one of its affiliates."
>
> "We provide personal information to our partners that provide product and service offerings or technologies that we think may be of interest to you."
>
> "In connection with purchases of certain Digital Content, we may need to forward information about you (including, for example, your Internet Protocol (IP) address) to the Digital Content provider in order to enable you to download or purchase Digital Content from or through that provider."
>
> *See* barnesandnoble.com Privacy Policy *infra* Appendix II.

98. *See* barnesandnoble.com (knowledgeable users) Survey Question 7 (on file with author).

99. *See, e.g.*, lowes.com Survey Question 9 (knowledgeable users) (on file with author); wunderground.com Survey Question 9 (knowledgeable users) (on file with author); washingtonpost.com Survey Question 9 (experts) (on file with author).

100. *See, e.g.*, lowes.com (experts and knowledgeable users) Survey Question 9 (on file with author). Notably, when asked if the website permitted users to delete their personal data, two experts answered "unclear," one "partial removal," and one "not applicable." Knowledgeable users expressed similar uncertainty in their answers to this question, with four knowledgeable users answering "unclear" while one answering "not applicable." Survey Question 9 (on file with author).

with respect to the privacy policy for Washington Post, three knowledgeable users selected that it was unclear if personal data was retained, while two answered that the question was not applicable and not addressed by the policy at all.[101] Similarly, three out of four experts selected "unclear."[102] In the washingtonpost.com example, most of the annotators chose the statement "[i]f you do not wish to receive the foregoing and therefore unregister from the site, please contact Customer Care and ask to have your registration account deleted."[103] This statement, however, was in reference to deleting a "registration account" in order to stop receiving items from the website such as legal notices and users' account statuses. This passage was not directed toward the true inquiry of whether or not the website would retain user data for other purposes in the future, and the annotators' responses reflected this ambiguity.

iv) Assumptions for the Interpretation of Specific Textual Language

Expert and knowledgeable users also made interpretative assumptions about the meaning of policy language. One interpretive difference arose in the context of permissive or conditional language. For example, annotators did not always interpret the word "may" in a policy in the same way. This was illustrated in some cases where experts selected the same text but chose different answer options.[104] This trend applied to both expert and knowledgeable users.[105]

101. *See* washingtonpost.com (knowledgeable users) Survey Question 9 (on file with author).

102. *See* washingtonpost.com (experts) Survey Question 9 (on file with author).

103. *See* washingtonpost.com Privacy Policy *infra* Appendix V.

104. *See, e.g.*, wunderground.com Survey Question 2 (on file with author). There, in response to a question about whether the website collects financial information, both annotators selected text that contained the following phrase: "companies that operate our online WunderStore, that process credit card information." *See* wunderground.com Privacy Policy *infra* Appendix VI. One annotator, in addition to selecting that phrase, selected the following language preceding it: "These Third Party Processors may include, for example," and likely interpreted this permissive language as rendering the language unclear (which corresponds to the answer option s/he selected). *Id.* The other annotator, however, did not select this permissive language. Instead, the annotator likely interpreted it to mean that permissiveness means actual practice, and thus chose Answer Option 2 ("Yes—the policy explicitly states that the website might collect financial information") (on file with author).

105. *See, e.g.*, lowes.com Survey Question 5 (on file with author). Three knowledgeable users selected "unclear" when asked if the privacy policy allowed the website to collect users' contact information. This is likely due to the permissive language of the privacy policy, which stated that the website "may share personal information we collect on the Site with certain service providers, some of whom may use the information for their own purposes." *See* lowes.com Privacy Policy *infra* Appendix III.

Another similar divergence of interpretative assumptions arose with respect to "sharing for core service." In at least one instance, the experts made different assumptions with respect to the scope of certain language. One annotator believed that third-party services that "operate [the] online WunderStore" or "process credit card information" to support the website fell outside the scope of "core service," while others did not.[106] Knowledgeable users, too, seemed to differ on their interpretations of what constituted a "core service." Divergent answer choices for a privacy policy that described third parties as "performing a service" for the website, when the nature of the services were not connected to the user's interaction with the website, highlighted this confusion.[107]

106. *See* wunderground.com Survey Question 6 (on file with author). There, two annotators selected the sentence: "These Third Party Processors may include, for example, companies that operate our online WunderStore, that process credit card information or handle shipping for Weather Underground." *See* wunderground.com Privacy Policy *infra* Appendix VI. One annotator selected the whole sentence along with Answer Option 3 to notate that "the policy states that the website might share financial information with third parties for other purposes." *Id.* The other annotator selected only the dark portion with Answer Option 2 to notate that "the policy explicitly states that the website might share financial information with third parties, but only for the purpose of providing a core service." *Id.*

107. *See* overstock.com Privacy Policy *infra* Appendix IV:

> Service Providers
>
> We may share information with companies that provide support services to us (such as a printer, e-mail, mobile marketing, or data enhancement provider) or that help us market our products and services. These companies may need information about you in order to perform their functions. These companies are not authorized to use the information we share with them for any other purpose.

Two out of five knowledgeable users selected the above passage to support their selection that that the website shared contact information "for core service only." All remaining annotators selected the same sentences. However, two of the remaining annotators selected that the website shared user information "for other purposes." The final remaining annotator selected "unclear." The answers from the overstock.com survey suggest that two out of five knowledgeable users have been influenced by the phrases "service providers" and "support services" when they selected the option "sharing for core service only." Though these phrases seem to indicate that sharing would occur for reasons directly related to users' immediate business with overstock.com, the end of the passage shows that this may not be the case. The final phrase "mobile marketing," which is listed as a third example of sharing,

The experts also made different assumptions for the interpretation of "unclear" as described in the answer option choices. For example, in one response to the question about whether the website would share contact information with third parties, two experts selected the following:

> As part of our ongoing partnership with Microsoft Corporation ("Microsoft"), we may share your personal information with Microsoft and its affiliates and subsidiaries under certain circumstances.[108]

However, one of the two experts who selected the text chose Answer Option 3 to reflect that "the policy states that the website might share contact information with third parties for other purposes." The other expert selecting the same text chose Answer Option 5 ("unclear"), defined as: "the policy does not explicitly state whether or not the website might share contact information with third parties, but the selected sentences could mean that contact information might be shared with third parties." The second expert likely selected the "unclear" option because of the assumption that "personal information" did not mean or include "contact information."

The knowledgeable users appear to have similarly diverged in their assumptions for the interpretation of "unclear." This divergence may particularly be seen in connection with questions about the collection of users' health information. None of the privacy policies reviewed by the group contained an explicit reference to health information. However, knowledgeable users were often divided on whether or not such collection was possible.[109] For example, in one survey, three knowledgeable users believed that it was "not applicable" to ask whether the privacy policy permitted collection of users' health information. The description for this answer choice stated that "this question is not addressed by this policy."[110] Yet, two knowledgeable users believed that it was "unclear" whether or not health information was collected. These users selected the statement "[w]e collect the following categories of information," which was later defined as "[i]nformation you provide in public forums on our sites and applications" and "[i]nformation sent either one-to-one or within a limited group using our message, chat, post or similar functionality."[111] These users likely picked

---

> demonstrates that contact information may in fact be shared for advertising purposes.

108. *See* barnesandnoble.com Privacy Policy *infra* Appendix II; Responses to Survey Question 5 (on file with author).

109. *See, e.g.*, lowes.com Responses to Survey Question 4 (on file with author).

110. *See* abcnews.go.com Response to Survey Question 5 (on file with author).

111. *Id.*

"unclear" because they read the policy language as ambiguous and as including the possibility that health information would be within the scope of data collection.

Finally, the experts sometimes differed in their interpretations of policy language if inferences could be drawn regarding a website's practices. For example, with respect to the collection of financial information, one expert selected the choice stipulating "the policy does not explicitly state whether the website might collect financial information or not, [but] the selected sentences could mean that financial information might be collected" and assumed that the selected text meant the website might collect financial information.[112] The expert was, in effect, responding on the basis of an assumption about the scope of a term in the policy. As it turned out, the policy contained explicit language about the collection of financial information so the assumption was correct.[113]

c) Human Error

Experts appeared to make human errors with occasional instances of mistake. In some cases, experts inadvertently focused on irrelevant material. For example, in response to the question "Does the policy state that the website might collect contact information," one expert annotator selected explicit language from a policy's "Types of Information We Collect" section, while another expert annotator focused instead on the policy's section "WE COLLECT INFORMATION WHEN" and selected language that did not seem to be an appropriate response to the question.[114]

---

112. *See* overstock.com Survey Question 2 (on file with author). One expert selected the following pieces of text to come to their conclusion:

> "You purchase, order, return, exchange or request information about our products and services from the Sites or mobile applications."
>
> "Product and Service Fulfillment"
>
> "Fulfill and manage purchases, orders, payments, returns/exchanges, or requests for information, or to otherwise serve you"

See overstock.com Privacy Policy *infra* Appendix IV.

113. *See* overstock.com Survey Question 2 ("What Information We Collect[:] . . . Your credit/debit card number.").

114. One expert selected the following language from the "Types of Information We Collect" section of overstock.com's privacy policy:

> Your name
> Your billing and delivery address
> Your e-mail address
> Your phone (or mobile) number

See overstock.com Survey Question 1 (on file with author). Another annotator selected the following language from the same policy's "We Collect Information When" section:

In a few other instances, experts simply made mistakes, as reflected by contradictory choices. As an illustration, one expert chose an answer option that should have been selected only if the accompanying passage mentioned "explicit consent"; the accompanying text passage, however, made no such mention.[115] Similarly, in response to a data deletion question, one expert selected an answer choice that should have been chosen if the accompanying selected text mentioned that a user's data might be retained even after a request that it be deleted; yet, the accompanying selected text did not mention retention.[116] It is unclear whether these occurrences resulted from

> You purchase, order, return, exchange or request information about our products and services from the Sites or mobile applications.
> You create an Overstock.com account
> You connect with Overstock.com regarding customer service via our customer service center, or on social media platforms.
> You visit the Sites or participate in interactive features of the Sites or mobile applications.
> You use a social media service, for example, Overstock.com's Facebook page or YouTube channel.
> You sign up for e-mails, mobile messages, or social media notifications from Overstock.com.
> You enter a contest or sweepstakes, respond to one of our surveys, or participate in a focus group.
> You provide us with comments, suggestions, or other input

See overstock.com Privacy Policy *infra* Appendix IV.

115. *See* wunderground.com Survey Question 5 (on file with author). Here, one expert annotator selected Answer Option 4, which reads: "Sharing for other purpose (explicit consent)—the policy explicitly states that the website might share contact information with third parties for a purpose that is not a core service, but only if the user provided explicit permission/consent to do so." The annotator selected the following text to accompany this answer choice:

> [W]e may share demographic information, location data, IP address, aggregate (not individual) usage statistics for our Services, other identifiers and information with advertisers and other third parties. For example, we may share IP address, random or anonymous device identifier, city and state, ZIP code, and specific geo-location with the parties identified in subparagraph F below.

See wunderground.com Privacy Policy *infra* Appendix VI. This selection mentions sharing "for a purpose that is not a core service," but does not require explicit user consent for the sharing it describes.

116. *See* washingtonpost.com Survey Question 9 (on file with author). Here, one expert annotator selected Answer Option 3, which reads: "Partial Removal - the policy explicitly states that users may delete their personal data but some/all of the data might be retained for other purposes, whether the data was provided directly by the user, generated by the user's activities on the website, or acquired from third parties." That annotator selected the following policy text, which makes no reference to data retention: "If you do not wish to receive the foregoing and therefore unregister from the site, please contact Customer Care and ask to have your registration account deleted. Once your account has been deleted, you

mistaken language selection, mistaken answer option selection, or other factors.

Lastly, experts occasionally missed relevant passages and selected a different portion of text that also accurately responded to the question asked. In these instances, each of the experts could have *also* selected the text that another expert selected.[117] This qualifies as a "mistake" because one expert missed relevant language that another saw. This example reveals that privacy policies can be confusing to a degree that even privacy policy "experts" have difficulty recognizing a policy's full scope. Ultimately, however, these "mistakes" will likely have little effect on adequately informing the NLP tool despite the experts' differences, as the data used to inform the tool will contain both selections. These examples, though, suggest that crowdsourcing

will no longer have access to washingtonpost.com, however, you may reregister at any time." *See* washingtonpost.com Privacy Policy *infra* Appendix V.

117. *See*, for example, Survey Question 4 regarding collection of health information for the abcnews.com Privacy Policy (on file with author). In response, two experts selected Answer Option 3, which reads: "Unclear—the policy does not explicitly state whether the website might collect health information or not, but the selected sentences could mean that the health information might be collected." To accompany this selection, one annotator chose one string of text ("Information you provide in public forums on our sites and applications[,] Information sent either one-to-one or within a limited group using our message, chat, post or similar functionality, where we are permitted by law to collect this information"), while the other selected a completely different string ("We acquire information from other trusted sources to update or supplement the information you provided or we collected automatically"). *See* abcnews.com Privacy Policy *infra* Appendix I. In this instance, both annotators could have selected both strings of text.

Another example can be seen in Survey Question 4 for the lowes.com Privacy Policy. There, in response to a question of whether the website might share contact information, one annotator selected option 3 ("Sharing for other purpose—the policy states that the website might share contact information with third parties for other purposes. The policy makes no statement about the users [sic] consent/permission or user consent is implied."), and another selected answer option 5 ("Unclear—the policy does not explicitly state whether the website might share contact information with third parties or not, but the selected sentences could mean that contact information might be shared with third parties."). Again, here, the annotators selected different language supporting each answer choice. One annotator (the one who chose option 5) selected, among others, the following string of text: "We may share personal information we collect on the Site with certain service providers, some of whom may use the information for their own purposes." *See* lowes.com Privacy Policy *infra* Appendix III. The other annotator (choosing answer option 3) selected this text: "We reserve the right to transfer personal information we have about you in the event we sell or transfer all or a portion of our business or assets (including, without limitation, in the event of a reorganization, dissolution or liquidation). Should such a sale or transfer occur, we will use reasonable efforts to direct the transferee to use personal information you have provided to us in a manner that is consistent with our Privacy Statement." *See* lowes.com Privacy Policy *infra* Appendix III. Again, each annotator could have selected the text that the other selected.

solutions may help remedy some of the human errors made while interpreting policies.

V. SIGNIFICANCE OF FINDINGS

Discrepancies between privacy experts and law and policy researchers reveal areas for careful attention to the quality of privacy policies. Discrepancies between privacy experts and non-expert users cast doubt on whether website notices, as they are typically worded today, can effectively convey privacy policies to the general public. If websites are not effectively conveying privacy policies to consumers in a way that a "reasonable person" could understand, notice and choice fails as a framework. If consumers cannot successfully decode privacy policies, the underpinnings of the U.S. approach to privacy are unsustainable, and regulation may be necessary. Indeed, a gap in interpretation between expert and typical users indicates that privacy policies are in fact misleading the general public and that those policies could be considered legally unfair and deceptive if the gap is intentional.

This Section will address some of the implications from the findings for common understandings of website privacy policies and for crowdsourcing the interpretation of privacy policies.

A. IMPLICATIONS FOR COMMON UNDERSTANDING AND CONSUMER DECEPTION

The findings show a number of areas where website privacy policies are too ambiguous to be meaningful and reveal a need to clarify specific data practices. The research demonstrates that policies describe websites' data sharing practices poorly. Experts could not reach consensus on interpretation of data sharing practices generally and agreed *even less* as to the various nuances of data sharing.[118] Website owners must be more candid and clear in drafting notices of data sharing practices. In particular, more precision is needed with respect to the collection of specific types of users' personal information. The findings showed common understandings among experts on contact and location information, but not on financial and health information.[119] This indicates that more clarity is necessary to spell out websites' specific practices with respect to sensitive information (i.e., financial and health information). General statements concerning "personal

118. *See supra* Table 2.
119. *See supra* Table 1.

information" often introduce ambiguity into a policy and makes it difficult to interpret which information the website is actually collecting.

The findings also showed many instances where a majority of non-expert users interpreted terms differently from experts.[120] This implies that website notices are not conveying accurate information to consumers and that privacy policies may be misleading the public in specific areas. For example, knowledgeable users and crowd workers both lagged substantially behind the experts in their understanding of websites' data practices.[121] Conversely, there were instances when experts could not agree on an interpretation, but non-experts users did agree on the interpretation. This may indicate that some language in website notices are commonly misunderstood where non-expert readers fail to recognize the ambiguity in a site's stated practices. For instance, when policies are silent on specific issues, or when conditions of sharing with third parties are not described clearly, non-experts will have a tendency to misunderstand the terms.

Lastly, since the findings reveal that complete agreement was uncommon, even among experts, website policies may be difficult to interpret through automated means. In other words, where users are unable to understand the policies accurately, automated tools will similarly misapprehend policy language. These difficulties are most pronounced at the level of specific practices. In instances where there is consensus on how data is treated *broadly*, for example, whether a policy states that a user may delete his or her personal information generally,[122] confusion increases exponentially when more nuance exists as to the data practice—such as instances when a policy provides for the ability to *fully* or *partially* delete user information.[123] This difficulty applied to each group of annotators. This disparity is very significant because personal privacy preferences are contextually based.[124] To have contextual integrity, the granular aspects of a data practice, not just whether a website collects, shares, or deletes personal information in general, will need to be understandable to a user. Indeed, a policy statement acknowledging general data collection and/or sharing may do very little to inform readers about the practices relevant for the user.

120. This arises when experts reach a *unanimous* consensus, yet a majority of non-experts interpret the same terms differently.

121. *See supra* Table 5.

122. *See supra* Table 3.

123. *See supra* Table 3.

124. *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRITY OF SOCIAL LIFE (2009).

The lack of agreement among users and the difficulties they have interpreting policies suggest that consumers are currently misled by website privacy policies. To the extent that vague and misleading terminology is the result of drafting errors and omissions, this research shows areas where website policies can and need to be improved. To the extent, however, that vague and misleading terms are intentionally introduced into website privacy policies, this research suggests that websites are successfully deceiving consumers. The Federal Trade Commission under its unfair and deceptive practice jurisdiction, and private litigants under state unfair and deceptive practice laws, may be able to address such deficiencies in enforcement proceedings.[125]

B. IMPLICATIONS FOR CROWDSOURCING

Semi-automated extraction of meaning from website privacy policies may, in some circumstances, be a solution to help solve the difficulties users face in the interpretation and comprehension of privacy policies. Crowdsourcing is a critical part of such extraction and the findings of this research raise a number of implications for crowdsourcing opportunities. These implications arise from cases in our study when experts agree on the interpretation of terms in the privacy policies and when experts disagreed on interpretation.

1. When Experts Agree

Where there is intra-group agreement among experts, then it is possible to compare the crowdsourced majority answer to the expert-selected answer to see whether a majority of crowd workers are able to arrive at the "correct" answer. Crowd workers in our study did a reasonable job predicting the answer when the experts had intra-group agreement. For example, experts had a high level of intra-group agreement with respect to the collection of location information[126] and, at the same time, the majority of crowd workers chose the same response as the experts, signifying that both groups interpreted the collection of location information in the same way.[127] This alignment between experts and crowd workers on the interpretation suggests that crowdsourcing could be leveraged to identify collection practices for certain types of data in privacy policies, i.e., those in our study where

125. For a discussion of these types of enforcement actions, see PRIVACY ENFORCEMENT ACTIONS, *supra* note 71.

126. *See supra* Table 1.

127. *See supra* Table 4.

agreement between experts and crowd workers indicates that the two groups' interpretations are very close.

By contrast, where there is intra-group agreement among experts and crowd workers fail to arrive at the experts' "correct" answer, then crowd workers misunderstand policy terms. For example, experts were largely in agreement on whether websites collected financial information,[128] but the majority of crowd workers failed to select the experts' answer.[129] This inconsistency suggests that extracting information practices for these types of data cannot easily be crowd sourced to typical users because their interpretation of the policy is likely to be wrong compared to the experts' interpretation.[130]

2. When Experts Disagree

Crowd workers, also, show positive signs at predicting expert disagreement. For example, neither experts nor crowd workers could agree on whether websites shared location information.[131] This suggests that crowd worker disagreement might serve as a proxy for expert disagreements and that those disagreements can be used to identify aspects of, and potentially specific passages within, websites' privacy policies that lack adequate precision.

By contrast, when experts disagree but the majority of crowd workers do choose an answer, the crowd workers may either be misunderstanding the policy or interpreting the survey questions differently from the experts. For example, experts had low intra-group agreement on whether websites shared health information[132] and did not agree completely on the best answer choice.[133] Yet, crowd workers all converged on the same response to the

128. *See supra* Table 1.

129. *See supra* Table 4.

130. At the same time, one natural language processing technique might be used to recognize text patterns in the policy that prompted experts' answer choices and then build crowdsourcing tools that combine machine learning and natural language processing techniques to improve the performance of crowd workers. The results of an automated extraction would be shown to crowd workers, for whom it may then be easier to verify the correctness of an extracted data practice or be less influenced by other text as compared to identifying the data practice correctly without assistance. The possibility remains to be studied. Another possible opportunity for enhancing the effectiveness of crowd workers and the accuracy of their extractions is to train them with example annotations provided by experts or knowledgeable users.

131. *See supra* Table 2. Experts were divided on the sharing of location information with a median level of agreement on all answer choices at 62.5%. Crowd workers had a median level of agreement at 40%.

132. *See supra* Table 2.

133. *See supra* Table 5.

sharing question.[134] In a case like this, there appear to be two possible explanations. First, the crowd workers might be failing to see the ambiguity in the policy and consequently would be misunderstanding the terms. Alternatively, as reflected in the qualitative findings, the two groups might be interpreting the questions and answer choices differently.[135]

These issues require further exploration to inform whether and how crowdsourcing tasks might be organized in support of semi-automated privacy policy annotation to achieve replication of expert interpretations.[136] Similarly, further exploration will be necessary to identify whether and how to augment crowdsourcing with combinations of NLP techniques and machine learning. Our study strongly suggests, however, that for a narrow range of data practices, both crowdsourcing and automated extraction may be within reach. For other data practices, such as information sharing with third parties, where policies are sufficiently ambiguous to cause disagreement between experts, further research will be required to address the challenges of devising crowdsourcing tasks and automated extraction that would enable non-experts to accurately determine a policy's interpretation.

VI. CONCLUSIONS

The results of this study have significant implications for public policy and technological developments. The disagreements among experts as reflected in the intra-group findings[137] demonstrate that privacy policies are ambiguous on key terms. Specifically, the findings show interpretative challenges with respect to certain types of information, the scope of data sharing, and the scope of data deletion rights. The findings also show that both knowledgeable users and crowd workers had greater difficulty deciphering privacy policy language than the experts.[138] Taken together, these findings suggest that privacy policies are written ambiguously and in a way that leads both knowledgeable users and crowd workers to misapprehend websites' data practices as well as cause disagreement among experts with respect to certain data practices.

If the ambiguity in website privacy policies is unintentional, then the findings illustrate where businesses need to improve the clarity of their website privacy policies. The study methodology may also enable industry-

134. *See supra* Table 5.

135. *See* Subsection IV.C.2.a)

136. For an experimental approach towards refining a workflow of crowdsourcing tasks for extracting data practices from privacy policies, see Breaux & Schabu, *supra* note 62.

137. *See supra* Sections IV.A, C.2.

138. *See supra* Sections IV.C.1.

wide tracking of how business sectors adjust their policies to more clearly explain their information practices. Specifically, web sweeps on a periodic basis to collect privacy policies as discussed in Section III.B would provide a data set to examine the evolution of privacy policies by industry sectors over time. Then, to the extent that some data practices can be extracted from crowdsourcing, and eventually natural language processing, these techniques could identify if privacy policy terms change over time.

If, however, the ambiguity is intentional, then the study findings suggest that website policies deceive the public. Such deception would be ripe for investigation by the Federal Trade Commission as "unfair and deceptive" business practices.

For the development of automated and crowdsourcing technological tools to assist end-users and policymakers in understanding privacy policies, the findings show initial promise as well as a need for further research into the important, identified challenges.[139] Machine learning and natural language processing techniques might be useful to highlight potentially relevant passages in a privacy policy for crowd workers who are trying to extract information about that practice. Our findings further suggest that crowdsourcing can be used today to infer some aspects of the meaning of textual statements and that these interpretations may be used to code for the automatic extraction of answers from those passages. Where crowd workers can predict expert disagreement about the interpretation of policy language, those ambiguous passages might be parsed out. For the remaining policy text, crowd workers' success in predicting answers where experts would agree may be used to code passages where there is interpretative agreement. This approach may thus provide a more accurate understanding of the legal meaning of some of the privacy policy terms where an individual, non-expert user would otherwise be misled. However, given a high level of actual disagreement among experts or crowd-predicted disagreement among experts, significant and important terms in privacy policies will very likely escape effective interpretation by crowd workers because the effectiveness of automated tools and crowdsourced interpretation depends on an accurate baseline meaning for text in a privacy policy. Such baseline meaning is currently missing for some of the key attributes of the website policies that were analyzed in this study.

139. *See* Sadeh et al., *supra* note 2 (describing the importance of this research for natural language processing and crowdsourcing).

APPENDIX I:

PRIVACY POLICIES*

I. ABCNEWS.GO.COM

The Walt Disney Company has a rich tradition of bringing great stories, characters and experiences to our guests around the world, and our sites and applications are created to entertain and connect guests with the best that we have to offer on the platforms and devices our guests prefer.

Our privacy policy is designed to provide transparency into our privacy practices and principles, in a format that our guests can navigate, read and understand. We are dedicated to treating your personal information with care and respect.

Privacy Policy

TRUSTe online privacy certification
Last Modified: December 30, 2013

This privacy policy describes the treatment of information provided or collected on the sites where this privacy policy is posted. It also explains the treatment of information provided or collected on applications we make available on third-party sites or platforms if disclosed to you in connection with use of the application. We follow this privacy policy in accordance with local law in the places where we operate.

Types of Information We Collect
How We Collect Your Information
Use of Your Information by The Walt Disney Family of Companies
Sharing Your Information with Other Companies
Your Controls and Choices

---

* These privacy policies are the versions used in this study as collected from the websites of companies. The policies in this appendix do not have the same formatting as the originals found on the websites. The table of contents, the alphabetical organization and some of the heading fonts were added to allow for faster navigation. No changes were made to the text of any of the policies.

TYPES OF INFORMATION WE COLLECT

We collect two basic types of information - personal information and anonymous information - and we may use personal and anonymous information to create a third type of information, aggregate information. We collect the following categories of information:

Registration information you provide when you create an account, including your first name and surname, country of residence, gender, date of birth, email address, username and password
Transaction information you provide when you request information or purchase a product or service from us, whether on our sites or through our applications, including your postal address, telephone number and payment information
Information you provide in public forums on our sites and applications
Information sent either one-to-one or within a limited group using our message, chat, post or similar functionality, where we are permitted by law to collect this information
Information you provide to us when you use our sites and applications, our applications on third-party sites or platforms such as social networking sites, or link your profile on a third-party site or platform with your registration account
Location information when you visit our sites or use our applications, including location information either provided by a mobile device interacting with one of our sites or applications, or associated with your IP address, where we are permitted by law to process this information
Usage, viewing and technical data, including your device identifier or IP address, when you visit our sites, use our applications on third-party sites or platforms or open emails we send
back to top of page

HOW WE COLLECT YOUR INFORMATION

We collect information you provide to us when you request products,

services or information from us, register with us, participate in public forums or other activities on our sites and applications, respond to customer surveys, or otherwise interact with us. Please keep in mind that when you provide information to us on a third-party site or platform (for example, via our applications), the information you provide may be separately collected by the third-party site or platform. The information we collect is covered by this privacy policy and the information the third-party site or platform collects is subject to the third-party site or platform's privacy practices. Privacy choices you have made on the third-party site or platform will not apply to our use of the information we have collected directly through our applications.
We collect information through technology, such as cookies, Flash cookies and Web beacons, including when you visit our sites and applications or use our applications on third-party sites or platforms. Please visit Online Tracking and Advertising for further information, including Do Not Track and how to disable cookies.
We acquire information from other trusted sources to update or supplement the information you provided or we collected automatically. Local law may require that you authorize the third party to share your information with us before we can acquire it.
back to top of page

USE OF YOUR INFORMATION BY THE WALT DISNEY FAMILY OF COMPANIES

A member of The Walt Disney Family of Companies, which includes many different brands, will be the data controller for your information. The relevant data controller(s) can be determined here. Other members of The Walt Disney Family of Companies may have access to your information where they perform services on behalf of the data controller(s) (as a data processor) and, unless prohibited under applicable law, for use on their own behalf (as a data controller) for the following purposes:

Provide you with the products and services you request
Communicate with you about your account or transactions with us and send you information about features on our sites and applications or changes to our policies
Consistent with local law and choices and controls that may be available to you:
Send you offers and promotions for our products and services or third-party products and services
Personalize content and experiences on our sites and applications
Provide you with advertising based on your activity on our sites and applications and on third-party sites and applications. To learn more about

how we use your information for personalization and tracking, please visit Online Tracking and Advertising.
Optimize or improve our products, services and operations
Detect, investigate and prevent activities that may violate our policies or be illegal
back to top of page

SHARING YOUR INFORMATION WITH OTHER COMPANIES

We will not share your personal information outside The Walt Disney Family of Companies except in limited circumstances, including:

When you allow us to share your personal information with another company, such as:
Electing to share your personal information with carefully selected companies so that they can send you offers and promotions about their products and services
Directing us to share your personal information with third-party sites or platforms, such as social networking sites
Please note that once we share your personal information with another company, the information received by the other company becomes subject to the other company's privacy practices.

When we cooperate with financial institutions to offer co-branded products or services to you, such as our co-branded Disney Rewards Visa Card; however, we will do so only if permitted by applicable law and, in these cases, the financial institutions are prohibited from using your personal information for purposes other than those related to the co-branded products or services
When companies perform services on our behalf, like package delivery and customer service; however, these companies are prohibited from using your personal information for purposes other than those requested by us or required by law
When we share personal information with third parties in connection with the sale of a business, to enforce our Terms of Use or rules, to ensure the safety and security of our guests and third parties, to protect our rights and property and the rights and property of our guests and third parties, to comply with legal process or in other cases if we believe in good faith that disclosure is required by law
back to top of page

YOUR CONTROLS AND CHOICES

We provide you the ability to exercise certain controls and choices regarding our collection, use and sharing of your information. In accordance with local law, your controls and choices may include:

You may correct, update and delete your registration account
You may change your choices for subscriptions, newsletters and alerts
You may choose whether to receive from us offers and promotions for our products and services, or products and services that we think may be of interest to you
You may choose whether we share your personal information with other companies so they can send you offers and promotions about their products and services
You may choose whether to receive targeted advertising from many ad networks, data exchanges, marketing analytics and other service providers here
You may request access to the personal information we hold about you and that we amend or delete it and we request third parties with whom we have shared the information do the same
You may exercise your controls and choices, or request access to your personal information, by visiting Communication Choices, contacting Guest Services, or following instructions provided in communications sent to you. Please be aware that, if you do not allow us to collect personal information from you, we may not be able to deliver certain products and services to you, and some of our services may not be able to take account of your interests and preferences. If you have questions regarding the specific personal information about you that we process or retain, please contact Guest Services.

back to top of page

CHILDREN'S PRIVACY

We recognize the need to provide further privacy protections with respect to personal information we may collect from children on our sites and applications. Some of the features on our sites and applications are age-gated so that they are not available for use by children, and we do not knowingly collect personal information from children in connection with those features. When we intend to collect personal information from children, we take additional steps to protect children's privacy, including:

Notifying parents about our information practices with regard to children, including the types of personal information we may collect from children, the uses to which we may put that information, and whether and with whom we may share that information
In accordance with applicable law, obtaining consent from parents for the collection of personal information from their children, or for sending information about our products and services directly to their children
Limiting our collection of personal information from children to no more than is reasonably necessary to participate in an online activity
Giving parents access or the ability to request access to personal information we have collected from their children and the ability to request that the personal information be changed or deleted
For additional information about our practices in the United States and Latin America regarding children's personal information, please read our Children's Privacy Policy.

back to top of page

DATA SECURITY AND INTEGRITY

The security, integrity and confidentiality of your information are extremely important to us. We have implemented technical, administrative and physical security measures that are designed to protect guest information from unauthorized access, disclosure, use and modification. From time to time, we review our security procedures to consider appropriate new technology and methods. Please be aware though that, despite our best efforts, no security measures are perfect or impenetrable.

back to top of page

DATA TRANSFERS, STORAGE AND PROCESSING GLOBALLY

We operate globally and may transfer your personal information to individual companies of The Walt Disney Family of Companies or third parties in locations around the world for the purposes described in this privacy policy. Wherever your personal information is transferred, stored or processed by us, we will take reasonable steps to safeguard the privacy of your personal information. Additionally, when using or disclosing personal information transferred from the European Union, we abide by the Safe Harbor Principles as set forth by the U.S. Department of Commerce, use standard contract clauses approved by the European Commission, adopt other means

under European Union law for ensuring adequate safeguards, or obtain your consent. We also apply the substantive requirements of the Safe Harbor Principles when transferring personal information from Australia.

back to top of page

CHANGES TO THIS PRIVACY POLICY

From time to time, we may change this privacy policy to accommodate new technologies, industry practices, regulatory requirements or for other purposes. We will provide notice to you if these changes are material and, where required by applicable law, we will obtain your consent.

back to top of page

COMMENTS AND QUESTIONS

If you have a comment or question about this privacy policy, please contact Guest Services. Our sites and applications may contain links to other sites not owned or controlled by us and we are not responsible for the privacy practices of those sites. We encourage you to be aware when you leave our sites or applications and to read the privacy policies of other sites that may collect your personal information.

Notice to California Residents: If you are a California resident, California Civil Code Section 1798.83 permits you to request information regarding the disclosure of your personal information by certain members of The Walt Disney Family of Companies to third parties for the third parties' direct marketing purposes. With respect to these entities, this privacy policy applies only to their activities within the State of California. To make such a request, please send an email to caprivacy.wdig@twdc.com or write us:

CA Privacy Rights
Disney Interactive
500 South Buena Vista Street
Mail Code 7667
Burbank, CA 91521-7667

In your request, please specify the member of The Walt Disney Family of companies to which your request pertains. If no member is specified, we will treat your request as pertaining to Disney Online.

back to top of page

DEFINITIONS

Aggregate Information. Aggregate information means information about groups or categories of guests, which does not identify and cannot reasonably be used to identify an individual guest.

back to top of page
Anonymous Information. Anonymous information means information that does not directly or indirectly identify, and cannot reasonably be used to identify, an individual guest.

back to top of page
Application. Application means a program or service operated by us (or on our behalf) that may be displayed on various online, mobile or other platforms and environments, including those operated by third parties, which permits us to interact directly with our guests.

back to top of page
Children. Children means individuals who we have identified are not of legal age to consent to the collection and processing of their personal information. In the United States and Latin America, the term "children" refers to individuals under 13 years of age.

back to top of page
Data Controller. The data controller is the subsidiary or affiliated entity of The Walt Disney Company that is responsible for the personal information collected from sites and applications, as follows:

Sites and Applications Company Contact Information
Disney Club Penguin ("Club Penguin") Disney Canada Inc. (formerly known as Disney Online Studios Canada Inc.) Club Penguin
c/o Disney Online Studios Canada Inc.
1628 Dickson Avenue, Suite 500
Kelowna, British Columbia V1Y 9X1
CANADA
support@clubpenguin.com
Disney Movies Online Disney Online, Buena Vista Home Entertainment, Inc. Disney Interactive
500 South Buena Vista Street

Mail Code 7667
Burbank, CA 91521-7667
United States of America
Guest Services
Disney Studio All Access
Disney Movie Rewards Disney Online, Buena Vista Home Entertainment, Inc., Walt Disney Studios Motion Pictures Disney Interactive
500 South Buena Vista Street
Mail Code 7667
Burbank, CA 91521-7667
United States of America
Guest Services
All other sites and applications Disney Online Disney Interactive
500 South Buena Vista Street
Mail Code 7667
Burbank, CA 91521-7667
United States of America
Guest Services
back to top of page
Data Processor. A data processor is a person or entity that processes personal information on behalf of a data controller (or data controllers) and is permitted to perform data processing only as directed by the data controller(s).

back to top of page
IP Address. An IP address is associated with the access point through which you enter the Internet, and is typically controlled by your Internet Service Provider (ISP), your company, or your university. We may use IP addresses to collect information regarding the frequency with which our guests visit various parts of our sites and applications, and we may combine IP addresses with personal information.

back to top of page
Member. Member means a subsidiary or affiliated entity that is part of The Walt Disney Family of Companies.

back to top of page
Notice. Notice may be by email to you at the last email address you provided us, by posting notice of such changes on our sites and applications, or by other means, consistent with applicable law.

back to top of page
Parents. Parents means a parent or legal guardian.

back to top of page
Personal information. Personal information means information that identifies (whether directly or indirectly) a particular individual, such as the individual's name, postal address, email address and telephone number. When anonymous information is directly or indirectly associated with personal information, this anonymous information also is treated as personal information.

back to top of page
Public Forums. Our sites and applications may offer message boards, conversation pages, blogs, chat rooms, social community environments, profile pages, and other forums that do not have a restricted audience. If you provide personal information when you use any of these features, that personal information may be publicly posted and otherwise disclosed without limitation as to its use by us or by a third party. To request removal of your personal information from a public forum on one of our sites or applications, please contact Guest Services.

back to top of page
The Walt Disney Family of Companies. The Walt Disney Family of Companies refers to The Walt Disney Company and its subsidiary and affiliated entities, which offer their products and services under various brand names. These companies engage in a number of businesses, including theme parks and travel, motion pictures and television, publishing, consumer products and interactive services. The Walt Disney Company brands include, among others, the following:

ABC
Babble
Baby Einstein
BabyZone
Club Penguin
Disney
Disney Pixar
ESPN
Hollywood Records
Indiana Jones
Lucasfilm

Marvel
Muppets
Playdom
Spoonful
Star Wars
Tapulous
Touchstone
back to top of page

GUEST SERVICES CONTACT INFORMATION

United States of America:

Guest Services
Disney Interactive
500 South Buena Vista Street
Mail Code 7667
Burbank, CA 91521-7667
United States of America
Guest Services

For questions related to children's privacy, you may also telephone Guest Services at (877) 466-6669.

Disney Interactive has received the TRUSTe Privacy Seal in the United States, signifying that this privacy policy and our privacy practices have been reviewed for compliance with the TRUSTe program listed on the validation page available when you click on the TRUSTe Privacy Seal. The TRUSTe program covers only those properties identified on the validation page. If you believe that Disney Interactive has not responded to your inquiry or your inquiry has not been satisfactorily addressed, you may contact TRUSTe here or the United States Federal Trade Commission through its online consumer complaint form available here

II. BARNESANDNOBLE.COM

Effective Date: May 7, 2013

This Privacy Policy applies to personal and other information that may be collected when you interact with the Barnes & Noble enterprise which consists of (a) Barnes & Noble, Inc. and its subsidiaries, including their

respective businesses and operations (collectively, "Barnes & Noble"); (b) businesses and operations managed or operated by Barnes & Noble; (c) websites owned, operated and managed by Barnes & Noble, including each website that links to this Privacy Policy, and any digital content stores operated by Barnes & Noble (collectively, "Barnes & Noble Websites"); and (d) Barnes & Noble's devices, content and applications. Protecting the privacy and security of your personal information is a priority at Barnes & Noble, and we believe that a single, comprehensive privacy policy that is straightforward and clear is in the best interests of our customers and our businesses. More detailed information about specific practices regarding Barnes & Noble and NOOK mobile devices ("Devices") and mobile applications developed and maintained by Barnes & Noble and NOOK ("Apps") is contained in the Barnes & Noble Mobile Privacy Supplement which is incorporated into, and subject to, this Privacy Policy. To review the prior version of Barnes & Noble's Privacy Policy, please click here.

By doing business with or interacting with Barnes & Noble in the manner described in this Privacy Policy at any time, you are accepting the practices described in this Privacy Policy and you consent to the application of this Privacy Policy to the collection, storage, use and disclosure of all your personal and other information as described.

Special Note: On October 4, 2012, Barnes & Noble underwent a corporate reorganization resulting in its digital and College businesses becoming owned by Barnes & Noble's majority owned subsidiary NOOK Media LLC and its subsidiaries (collectively "NOOK Media"). These current privacy policies and the privacy practices described herein apply to personal information previously collected from you by Barnes & Noble, Inc. and each of its subsidiaries, including NOOK Media, as well as personal information that they may collect from you in the future. Please be advised that NOOK Media intends to launch one or more of its own websites in the future for purposes of operating its digital and College businesses. NOOK Media expects to post privacy policies applicable to those websites when they are launched.

Barnes & Noble reserves the right to modify or amend this Privacy Policy at any time, but you can be assured that, should it be necessary to do so, we will always do so in accordance with the Barnes & Noble Privacy Principles of Clarity, Security and Integrity. You will be notified of any material changes to this Privacy Policy which are less protective of customer information prior to such changes becoming effective. We may notify you of these changes by

email reminders, by notice on this site, or by other acceptable means. We encourage you to periodically review this page for the latest information on our privacy practices.

Clarity: We strive to communicate clearly about your privacy and how we handle your personal information.
Security: We follow security standards, processes and procedures that are designed to protect your personal information.
Integrity: We do not sell or rent your personal information and respect your preferences with respect to your personal information.

Below you will find answers to the following frequently asked questions about how we collect, use and share your personal information:

1. What is the personal information that we collect?
2. Why do we collect personal information?
3. How do we collect your personal information?
4. How do we use personal information?
5. With whom do we share personal information?
6. How do we secure personal information?
7. How do we respect your choices about your personal information?
8. Whom do I contact if I have questions or concerns?
9. What other information about Barnes & Noble's Privacy Policy would I want to know?

1. WHAT IS THE PERSONAL INFORMATION THAT WE COLLECT? *

Depending on how you choose to interact with the Barnes & Noble enterprise, we may collect personal information from you, for example your name, e-mail address, billing address, shipping address, phone number, credit card information, date of birth and other persistent identifiers that can be used to personally identify you. If you rent, purchase or otherwise place orders for textbooks from Barnes & Noble College Booksellers, we may also collect your student or faculty identification number, financial aid number, your driver license number and information regarding courses you enroll in or teach. We may also collect other personal information regarding your interaction with Barnes & Noble Websites, Devices and Apps, including

* Numbers have been left in the Barnes & Noble privacy policy to reflect its original formatting, separate from BTLJ formatting.

usage information, the items that you browse, purchase, download, read, watch and otherwise access, and your geographic location. For further details about personal information collected through Apps and Devices, please read the Barnes & Noble Mobile Privacy Supplement.

2. WHY DO WE COLLECT PERSONAL INFORMATION?

We collect your personal information in an effort to provide you with a superior customer experience and, as necessary, to administer our business. It allows us to provide you with easy access to our products and services, with a particular focus on the items and programs that may be of most interest to you. For more information as to why we collect personal information, please see the section below entitled: "How do we use your personal information?"

Your personal information also allows us to communicate with you about special offers, promotions, and other marketing programs and news that may be of interest to you. You always have the opportunity to unsubscribe from promotional emails by following the instructions included in each marketing email or by changing your preferences in your account.

3. HOW DO WE COLLECT YOUR PERSONAL INFORMATION?

(a) Information that you provide to us

As a general matter, you can browse in our stores and on the Barnes & Noble Websites without submitting your personal information to us, although we may receive and collect certain personal information automatically, as outlined in Section 3(b) of this Privacy Policy, including site analytics regarding our websites, information your Internet browser automatically sends when you visit our websites, and information collected by cookies.

Making a purchase or placing an order
Creating an account or joining the Member Loyalty Program
Applying for a Barnes & Noble MasterCard
Signing up for Invite-a-Friend Emails
Using specific features of your Device
Contacting customer service
Additional Barnes & Noble Website, Device or App Features
Interacting with social networking sites
Entering a sweepstakes or contest

For your convenience, we have provided a summary description of each of these circumstances below.

Making a purchase or placing an order

When you make a purchase, rent or place an order in our stores, place an order online or purchase, download, rent or stream books, periodicals, movies, television shows and other digital content ("Digital Content"), you may need to submit personal information to us.

Creating an account or joining the Member Loyalty Program

In order to use Devices, certain Apps and features of Barnes & Noble Websites, or to purchase or access Digital Content, you may be required to create a password-protected user account and provide us with personal information when you do so. Similarly, when you enroll in our Member Loyalty Program, we will ask you to submit personal information as part of your member profile. We will store and use this information to administer the programs and services in which you choose to participate, and as permitted by this Privacy Policy.

Applying for a Barnes & Noble MasterCard

When you apply for a Barnes & Noble MasterCard, you will need to submit personal information directly to the issuer of the MasterCard. Personal information that you provide directly to the issuer is subject to the bank's privacy policies, practices and procedures, not Barnes & Noble's.

In addition, we disclose certain personal information to the issuer of the MasterCard in connection with the administration of the Barnes & Noble MasterCard program. The issuer does not have the right to use the personal information we provide beyond what is necessary to assist us or to administer this program. The issuer is contractually obliged to maintain the confidentiality and security of the personal information we provide and is restricted from using such information in any way not expressly authorized by us.

Signing up for Invite-a-Friend Features

Our Invite-a-Friend feature is located in various areas of certain Barnes & Noble Websites and within certain Devices. By clicking on 'Email' or 'Find friends from contacts' on your Device, customers can email a link to a friend which will invite the friend to view the Barnes & Noble Website page or attend the event described on that page.

The 'Find friends from contacts' feature on the Device may access the contacts you have entered into your Device in order to generate such emails. To remove yourself from these mailings, please call our Customer Service Center at 1-800-THE-BOOK (1-800-824-2665). Individuals calling from abroad should call us at 1-201-559-3882.

Using specific features of Barnes & Noble Websites, Devices and Apps

Barnes & Noble Websites, Devices and Apps may provide you with the ability to enter (either directly, or by authorizing Barnes & Noble to download the information from a third party such as a social networking website) your information such as your contacts, calendar entries or photos, or images you may submit to us to help us locate products for you. For further details about personal information collected through Devices and Apps, please read the Barnes & Noble Mobile Privacy Supplement.

Contacting Customer Service

When you contact customer service, we may ask you to provide, or confirm, personal information so that we can better serve you.

Additional Website, Device or App Features

From time to time we may offer or provide new or additional Barnes & Noble Website, Device or App features and functionality. Such features or functionality may request or require you to submit personal information to us in order to use such feature or functionality.

Entering a Sweepstakes or Contest

If you enter a sweepstakes or contest we offer, we may ask you to provide personal information so that we can consider your entry and, if you win, so that you may redeem your prize.

Interacting with Social Networking Sites

Our Devices and Apps may provide you with the ability to enter (directly, or by authorizing us to download the information from a third party such as a social networking site or application) personal information such as contacts or lists of friends. These or related applications may also allow you to provide information directly to social networking sites including information about your purchases, physical location, or comments. However, we will not provide any of your information to social networking sites without your express consent.

(b) Information automatically collected

There are circumstances in which we automatically receive and collect information from you. The most common sources of this information include:

Cookies
Pixel tags or clear Graphics Interchange Format files, known as GIFs
Your Device or Apps you use
Wireless networks operated by Barnes & Noble in retail stores
Business partners, contractors, shared databases, and other third parties who may occasionally share information with us, including UltraVioletâ„¢

For your convenience, we have provided a summary description of each of these circumstances below.

Information automatically collected when you visit Barnes & Noble Websites

When you visit a Barnes & Noble Website, we automatically record information that your browser sends us. For example, we may receive and collect: the name of the domain and host from which you access the Internet; the Internet Protocol (IP) address of the computer you are using; the date and time you access the Barnes & Noble Website; and the Internet address of the website from which you linked directly to the Barnes & Noble Website. We may also collect information regarding search queries run on the Barnes & Noble Website. We use this information to monitor the usage of the Barnes & Noble Websites and as necessary for our business.

Information collected using cookies

Like many online retailers, we and/or our third party providers use cookies to recognize you as you use or return to the Barnes & Noble Websites. This is done so that we can personalize and enhance your browsing and shopping experience. "Cookies" are small files that we place on your computer's hard drive to collect information about your activities on a Barnes & Noble Website. Cookies help us to: (1) speed navigation, keep track of items in your shopping bag and provide you with content that is tailored to you; (2) remember information you gave us so that you do not have to re-enter it; (3) determine the effectiveness of some of our and our third party partners' marketing efforts and communications; and (4) monitor the total number of visitors, pages viewed, and the total number of banners displayed.

Browsers are typically set to create cookies automatically. You can choose to have your browser notify you when cookies are being written to your computer or accessed, or you can disable cookies entirely. If you disable cookies, however, you will not be able to place items in a Barnes & Noble Website shopping bag, and therefore you will not be able to place an order with us online. Also, by not using cookies, some Barnes & Noble Website features and services may not function properly.

Additionally, we work with a third party service provider to help us better understand how you use the Barnes & Noble Websites. This third party service provider will place cookies on your computer to collect information such as how you were referred to the Barnes & Noble Website, how you navigated around the Barnes & Noble Website, what you purchased and what traffic is driven by banner ads and emails. This information will help us to better serve you and provide you with more personalized information and product offerings. We do not allow this third party service provider to collect your credit card information, e-mail address or password information. This third party service provider may only use your personal information to perform services for us and may not share your personal information with anyone else, or use it for any other purpose, except on an aggregated, non-personally identifiable basis. For more information, please view this third party's privacy policy.

You may choose to opt-out of this third party's analysis of your browsing and purchasing behavior on such Barnes & Noble Website. To do so, please click here.

By doing business with or interacting with Barnes & Noble, you consent to

the use of the tracking technologies as described above.

Information collected in connection with marketing e-mails and using pixel tags or clear GIFs

To help us understand the effectiveness of certain of our communications and marketing efforts, we may use sensing technologies that use pixel tags or clear GIFs (which are also called web beacons). These technologies allow us to determine the effectiveness of our e-mail and advertising and marketing efforts. For this purpose, we tie the pixel tags and clear gifs to personally identifiable information. We may also collect information regarding the links within such marketing materials that you click on and purchase statistics regarding items you buy following receipt of such marketing.

Information collected from Devices or Apps

When you use a Device or our Apps, we automatically collect information through the Device or App when it is connected to the Internet. For example, we may receive and collect information concerning device registration, settings, usage, firmware version, signal strength, search queries, network interaction, the name of the network from which you access the Internet, the Internet Protocol (IP) address of the device you are using, unique device identifiers (UDIDs), downloads, sideloaded content, configuration, or service information relating to any malfunction of the Device or App. This may include information regarding your reading or, in the case of videos, viewing behavior on such Devices or Apps, such as books or videos opened, page turns, bookmarks, annotations, or customer reviews.

In addition, to provide location-based services on Devices or through Apps, Barnes & Noble and third party application providers may automatically collect real-time geographic location information or other location-based information about you and your Device or other mobile device on which the App is installed. This information may be used to provide certain device or application functionality or to offer, provide and improve products and services.

For more information about information collected through Devices and Apps, please read the Barnes & Noble Mobile Privacy Supplement.

Information collected from outside sources

We may collect personal information and other information about you from business partners, contractors and other third parties. This includes, but is not limited to, instances in which you affirmatively authorize third parties to provide us with information. Such information may be collected via, but not limited to, software applications that you download or use on your Device or that otherwise allow you to interact with the Barnes & Noble enterprise. For example, if you link your UltraViolet account with your account with us, we may collect certain information regarding movies or television shows you have purchased from third parties as part of your UltraViolet collection of digital content.

If you rent or purchase textbooks from Barnes & Noble College Booksellers, we may also collect information about you from your college or university. This information may be used for a number of purposes including providing our services to you, sending postal mail and e-mail, fulfilling orders, removing repetitive or unnecessary information from customer lists, analyzing data, providing marketing support, customer authentication, providing search results and links (including paid listings and links), providing customer service and processing credit card payments.

Information collected from UltraViolet

If you link your account with us to your UltraViolet account, we may collect information regarding UltraViolet-enabled movies and television shows you have purchased from third party retailers. This will enable you to download or stream movies or television shows from us that you have purchased from us from such third parties. For more information, please view the UltraViolet privacy policy located at www.uvvu.com.

Information collected from visitors from outside the United States

If you are visiting Barnes & Noble or a Barnes & Noble Website from outside the United States and provide us with personal information, please note that your personal information will be transferred, stored and processed within the United States. Additionally, Barnes & Noble may transfer your personal information to other countries, for example because a server or third party service provider is located there. The data protection and privacy laws of other countries, including the United States, may not afford you the same level of protection as those in your own country. Barnes & Noble will take appropriate steps to protect your information.

By doing business or interacting with Barnes & Noble, you are consenting to the transfer, storage, and processing of your personal information to and within facilities located in the United States and other facility locations selected by Barnes & Noble.

4. HOW DO WE USE PERSONAL INFORMATION?

Barnes & Noble uses your personal information to provide you with a superior customer experience and, as necessary, to administer our business. For example, we use your personal information to:

Provide you with products, services and information, including product and subject recommendations and other information in Barnes & Noble retail stores, through e-mails from the Barnes & Noble enterprise, and on the Barnes & Noble Websites and online interactive communities, your Devices, Digital Content, Apps and software, and display associated content and advertising;

Administer our programs;

Provide customer service;

Conduct research and perform analysis in order to measure, maintain, protect, develop and improve our products and services;

Administer sweepstakes, contests, promotions or surveys and provide appropriate notifications;

Communicate with you about special offers, events, or new products or services that may be of interest to you;

Customize and enhance the Barnes & Noble Websites and advertising;

Make communications necessary to notify you regarding security, privacy, and administrative issues; and

Manage our business.

5. WITH WHOM DO WE SHARE PERSONAL INFORMATION?

Protecting the privacy and security of your personal information is a priority at Barnes & Noble. Barnes & Noble DOES NOT SELL OR RENT YOUR

PERSONAL INFORMATION TO THIRD PARTIES provided that your data may be transferred to or shared with a third party as part of a sale, merger, or acquisition of Barnes & Noble or one of its affilliates (see "Sales, Mergers, and Acquisitions" below).

Barnes & Noble shares your personal information with:

Other entities within the Barnes & Noble enterprise. Many of our customers purchase items from us both online and in our stores. In addition, Barnes & Noble owns and operates other operations and businesses and we share and use your personal information with our other business units and operations and may continue to do so even after such business units or operations are sold. We share your personal information within the Barnes & Noble enterprise (i) to help to ensure that you have a superior shopping or browsing experience no matter where you choose to shop or browse with us, (ii) to provide customer support and related services, (iii) to provide other services and products that might be of interest to you, (iv) to provide and/or manage certain cross-company promotions or programs (e.g. to honor your Barnes & Noble Member Program rewards), (v) to facilitate purchases of Devices or content (or other products) from within the Barnes & Noble enterprise, (vi) if we provide you with in store services and/or customer support for Devices and content, (vii) in connection with our commercial arrangements and business relationships within the Barnes & Noble enterprise, and (viii) as otherwise reasonably determined to provide a comprehensive retail and digital content experience for our joint customers.

Partners . We provide personal information to our partners that provide product and service offerings or technologies that we think may be of interest to you. Our partnerships may also result in products and services that allow you to publish Digital Content that may be shared with our partners. We may offer you the opportunity to opt-in to receive information from our partners, which may result in your personal information being shared with our partners. The use of your information by our partners and their vendors and contractors will be subject to the privacy policies of our vendors once such information is transferred.

Microsoft Corporation. As part of our ongoing partnership with Microsoft Corporation ("Microsoft"), we may share your personal information with Microsoft and its affiliates and subsidiaries under certain circumstances. If you consent to such sharing (including, without limitation, in connection with using a Microsoft account), Microsoft may use your personal

information to provide products and services to you related to your Device, Digital Content and Barnes & Noble and Microsoft services and products. These products and services may include, without limitation: (i) to enable purchases of Digital Content by you and provide Digital Content to you, (ii) to allow you to access, view and consume your Digital Content and provide related services to you, (iii) to publish certain Digital Content created by users and customers (as may be more fully set forth in any applicable terms or policies related thereto), (iv) to create and manage cross company user accounts and applications related to your Devices and Digital Content, including in connection with the integration between the Microsoft user and ID systems and Microsoft commerce platform and our products and services, (v) to offer joint product or service offerings, (vi) to provide customer support, (vii) to provide information to you regarding Microsoft product and service offerings, and (viii) as otherwise reasonably determined by us. Please note that any information provided to Microsoft will be treated by Microsoft in accordance with its applicable privacy policies in effect from time to time. Please refer to Microsoft's website for information related to Microsoft's collection, use and sharing of information that it obtains.

Service providers, subcontractors and agents who perform services on our behalf. We provide personal information to third party service providers, subcontractors, and agents that work under contract on our behalf to provide certain services. These third parties do not have the right to use personal information we provide to them in any way that is not authorized by Barnes & Noble. They are contractually obligated to use such information only as necessary to assist us and to maintain the confidentiality and security of such information.

Third party providers of products and services. These are third parties that provide products and services you may purchase or request from or through us. These third parties do not have the right to use personal information we provide to them in any way that is not authorized by Barnes & Noble. They are contractually obligated to use such information only as necessary to assist us and to maintain the confidentiality and security of such information.

UltraViolet. If you purchase UltraViolet-enabled movies or television shows from us, we may provide you with the opportunity to link your account with us to your UltraViolet account. This will enable you to download or stream movies or television shows that you have purchased from us from third party retailers who are part of the UltraViolet content ecosystem. For more information, please view the UltraViolet privacy policy located at

www.uvvu.com.

Third Party Membership Programs. We work with certain third party entities to help them administer their own membership or rewards programs by providing them with purchasing information about their customers who make purchase from Barnes & Noble. We disclose only the information that is necessary to make these third party programs work and to support your membership in them. This information usually includes your name and e-mail address as well as the dollar amount of the purchases made at Barnes & Noble. We require such entities to obtain your consent before we provide them with this information, which they usually do as part of their own membership or participation rules.

Credit Card Companies. Credit card transactions are handled by third party financial institutions and their vendors and contractors who receive credit card numbers and other personal information from us to verify the credit card numbers and process transactions. Although Barnes & Noble's treatment of this information is governed by this policy, the use of your information by the third party financial institutions and their vendors and contractors will be subject to their own privacy policies.

Law enforcement officials and as required by law. Barnes & Noble may release personal information to third parties when we determine, in our judgment, that it is necessary to (a) comply with the law, regulation, legal process, or enforceable governmental request; (b) enforce or apply the terms of any of our policies or user agreements; or (c) protect the rights, property or safety of Barnes & Noble, our employees, our customers, users, or others.

Co-branded offerings. In some instances, we may offer a service or feature that is co-branded by Barnes & Noble and a third party company. If you provide information in connection with such co-branded service or feature, that information may be shared between Barnes & Noble and the third party. Although Barnes & Noble's treatment of the information is governed by this policy, the third party's treatment of your information will be subject to the third party's privacy policy.

Other websites operated by Barnes & Noble. In some instances, we may operate a Barnes & Noble Website on behalf of a third party. If you provide information in connection with a Barnes & Noble Website operated by Barnes & Noble on behalf of a third party, that information may be shared between Barnes & Noble and the third party. Although Barnes & Noble's

treatment of the information is governed by this policy, the third party's treatment of your information will be subject to the third party's privacy policy.

Your college or university. Barnes & Noble College Booksellers may offer the ability to rent or purchase products or services through financial aid, student loans or similar programs. We may share your information with your college or university, lenders or other providers in order to process payments if you choose these payment methods.

Sales, Mergers, and Acquisitions. If Barnes & Noble becomes involved in a merger, acquisition, restructuring, reorganization, or any form of sale or other disposition of some or all of its assets, personal information and your transaction history may be provided to the entities and advisors involved subject to a confidentiality agreement, and we will provide notice to you at your email address on file before any personal information is finally transferred and becomes subject to a different privacy policy. Such a transaction may involve us (i) retaining the right to continue to use transferred personal information in addition to the right of the transferee to use such information, and (ii) engaging in additional transfers of personal information (including new personal information) with the transferee from time to time following such a transaction.

To Fulfill Your Requests For Products or Services

In connection with some Digital Content orders, in order to complete your transaction, we may need to forward your name, magazine, catalog or newspaper order, email address, and shipping or billing address to our content providers. The content providers will share your magazine, catalog or newspaper order information as well as your name and address, or name and e-mail and shipping or billing addresses with the magazine, catalog or newspaper publisher and magazine, catalog or newspaper circulation auditors. Magazine, catalog and newspaper publishers may use this information to fulfill your order and for other purposes. Your credit card information will not be shared with them.

In connection with purchases of certain Digital Content, we may need to forward information about you (including, for example, your Internet Protocol (IP) address) to the Digital Content provider in order to enable you to download or purchase Digital Content from or through that provider. In

each such instance, the Digital Content provider is obligated to use such information in accordance with its own privacy policy and applicable law.

6. HOW DO WE SECURE PERSONAL INFORMATION?

We take significant and appropriate security measures, including physical, technological and procedural measures, to help to safeguard your personal information and to prevent unauthorized access and disclosure. In addition, we use industry-standard technology, such as Secure Sockets Layer (SSL) encryption technology in the transmission of certain sensitive personal information, designed to prevent unauthorized persons from gaining access to your personal information, and, as technology develops, we intend to take additional measures to improve security.

We want you to feel confident whenever you visit us in our stores, on the Barnes & Noble Websites, or use Barnes & Noble Devices or Apps. While we are focused on the security of your personal information and follow strict standards, processes and procedures that are designed to protect your personal information, you must remember that the Internet is a global communications vehicle open to threats, viruses and intrusions from others and so we cannot promise, and you should not expect, that we will be able to protect your personal information at all times and in all circumstances.

7. HOW DO WE RESPECT YOUR CHOICES ABOUT YOUR PERSONAL INFORMATION?

When you interact with Barnes & Noble in certain ways, you may be eligible to receive certain marketing-related and promotional communications as well as special offers (collectively "Promotional Communications") from Barnes & Noble that may include advertisements from third parties. The most common of these circumstances include:

Making a purchase or download or placing an order
Creating an account
Joining a Barnes & Noble online community
Enrolling in our Member program
Signing up for Newsletters
Signing up with eBookstores operated by Barnes & Noble
Entering a sweepstakes or a contest

Where you have consented to receiving Promotional Communications from the Barnes & Noble enterprise, you may choose to opt-out at any time by

following the instructions below.

For Barnes & Noble Booksellers: At any time, a customer may choose to opt-out of the receipt of any promotional communications by clicking on the opt-out link provided at the bottom of each e-mail and following the instructions, or by e-mailing our Customer Service Department by clicking here.

For Barnes & Noble College Booksellers: At any time, a customer may choose to opt-out of the receipt of any promotional communications by clicking on the opt-out link provided at the bottom of each e-mail and following the instructions.

For barnesandnoble.com: Any account holder can opt-out of the receipt of any promotional communications by logging onto their Account and following the instructions under "Communication Preferences". If you do not have a barnesandnoble.com account, you may opt-out of the receipt of such communications by selecting the link at the bottom of any promotional e-mail communication and following the instructions.

For Barnes & Noble Member program: Any Member can opt-out of the receipt of any Member program promotional communications by logging on to their barnesandnoble.com Account and following the instructions under "Change Your Communication Preferences." If you do not have a barnesandnoble.com account, you may opt-out of the receipt of such communications by selecting the link at the bottom of any promotional e-mail communication and following the instructions.

For Barnes & Noble Educator program: Any Educator can opt-out of the receipt of any promotional communications by logging on to their barnesandnoble.com Account, clicking "Communication Preferences," and following instructions under "Change Communication Preferences." If you do not have a barnesandnoble.com account, you may opt-out of the receipt of such communications by clicking on the opt-out link provided at the bottom of each e-mail and following the instructions. If no opt-out link exists reply to the email with the word "Remove" in the subject line, or by e-mailing our Customer Service Department by clicking here.

For the Barnes & Noble Gift Card website: Any customer of the Barnes & Noble Gift Card website who receives promotional communications can

opt-out of the receipt of any such communications by clicking on the opt-out link provided at the bottom of each e-mail and following the instructions or by sending an e-mail to giftcardprefs@bn.com.

For SparkNotes.com: Any SparkNotes.com customer who does not wish to receive promotional product and service communications can choose to remove their contact information from SparkNotes.com contact list by following the instructions listed on www.sparknotes.com.

For Sterling Publishing: If, at any time, you wish to no longer receive ENewsletters from Sterling Publishing Co., Inc., Pixiq, Lark Crafts, and/or FlashKids.com, please click on the link for opt-out instructions contained at the bottom of each ENewsletter. You can change your personal information and your communication preferences when you follow this link.

Even if you opt-out of receiving Promotional Communications, you may continue to receive e-mails relating to order confirmations, back order notifications, membership information, and/or other business-related communications.

Note for Community Users

Barnes & Noble provides you with the ability to access, correct, change or request deletion of the personal information in your community profile(s) at any time by following the instructions below. We will respond to all access requests within 30 days. However, you cannot currently change your profile name although you may re-register and choose a new name. To review or modify your profile information, please click here. Please be advised that Barnes & Noble may archive information it collects on its community and visitors. Additionally, by participating in the Barnes & Noble online interactive community, and using Barnes & Noble's various interactive offerings, including, the submission of customer reviews, or participation in the Barnes & Noble Book Clubs, you agree to receive communications from Barnes & Noble, other users, and moderators related to the provision of these services.

You may access, correct or change the personal information in your community profile(s) on Lark Crafts and Pixiq at any time. To review or modify your profile information, log in to larkcrafts.com or pixiq.com. Additionally, by using Lark Crafts and/or Pixiq's various interactive

offerings, you agree to receive communications from Barnes & Noble, Lark Crafts, Pixiq, other users, and moderators related to the provision of these services.

You may also access, correct or change the personal information in your community profile(s) on SparkNotes.com at any time, except to change your username. To review or modify your profile information, log in to SparkNotes.com. Additionally, by using SparkNotes.com's various interactive offerings, you agree to receive communications from Barnes & Noble, SparkNotes, other users, and moderators related to the provision of these services.

We will retain your information for as long as your account is active or as needed to provide you with services. We will retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

8. WHOM DO I CONTACT IF I HAVE QUESTIONS OR CONCERNS?

If you have any questions about this Privacy Policy, please contact us at privacy@barnesandnoble.com or call customer service at 1-800-THE-BOOK [1-800-843-2665].

9. WHAT OTHER INFORMATION ABOUT BARNES & NOBLE'S PRIVACY POLICY WOULD I WANT TO KNOW?

Barnes & Noble Policies for Minors, including children under the age of 13.

Barnes & Noble is committed to complying with all applicable laws and regulations regarding the collection, storage and use of personal information of Minors under the age of 13, including the Children's Online Privacy Protection Act of 1998.

Except as noted below : (i) our products and services are marketed for and directed towards purchase by adults or with the consent of adults; (ii) Individuals under the age of 18 ("Minors") are not permitted to use Barnes & Noble Websites or Apps without the supervision of a parent or legal guardian; (iii) we do not knowingly collect or solicit personal information from children under the age of 13 or knowingly allow such persons to register for an online account or to post personal information on the Barnes & Noble Websites; and (iv) should we learn that someone under the age of 13 has provided any personal information to or on any of the Barnes &

Noble Websites, we will remove that information as soon as possible.

If we direct certain Devices features or Apps to Minors who may be under the age of 13, we require the parent or legal guardian to provide verifiable consent to such Minor's use of our products and services and our collection of personal information in connection with such use. In these cases, we require validation of credit card information already on file with us and we will then e-mail the master account holder to give notice that we have received such consent. If no credit card information is on file, or if the credit card is invalid, we will not register that you have consented. With your consent, we may collect, use and share information regarding Minors under the age of 13 consistent with this Privacy Policy. Please see the sections above for detailed information on how we do so.

If you are a parent or guardian who believes that your Minor under the age of 13 has submitted personal information or other information to us without your consent, please contact privacy@barnesandnoble.com. Once we verify that you are the parent or legal guardian, at your request, we will promptly provide to you information regarding what, if any, personal information we have collected about your child and how it has been used or shared. We will, at your request, remove personal information about your child from its database and instruct our affiliates and third party partners to do the same.

Your access rights and updates to your information

You have the right to ask us not to use your personal information for direct marketing purposes. You also have the right to request a copy of the personal information that we hold about you and to have any inaccuracies rectified. Please note that, as permitted by law, we may charge a nominal fee for information requests and may require you to prove your identity. Following a request, we will use reasonable efforts to supply, correct or delete personal information about you in our files. Please address written requests and questions about this to privacy@barnesandnoble.com. We will respond to all access requests within 30 days.

Third Party Applications: We are not responsible for third party applications you may download and install on your Devices. While Barnes & Noble uses reasonable efforts to ensure that applications offered through our Application Stores meet compatibility and safety testing criteria, this Privacy Policy does not cover any data collection, use, or sharing by mobile device manufacturers, network service providers or third party application

providers, unless such party has entered into a separate agreement with us as a business partner to share your personal information. In such a case, we would require our business partner to disclose their data collection and sharing practices with you, and obtain your prior affirmative consent. Our use of any shared data under such an agreement would then be governed by our privacy policy. All other collection of personal information by a third party application provider shall be subject to the terms of such provider's privacy policy.

Third Party Websites and Web-Tracking

We may partner with third party distributors of advertisements to deliver advertisements about our products and services when you visit other websites across the Internet. These distributors of advertisements may place or access cookies on your computer which help us provide you with advertisements that are customized to your particular product preferences and improve the effectiveness of our marketing efforts. If you would like to learn more about the third party advertisers that may be aware of the fact that you visit Barnes & Noble Websites, and to understand your choices about having such advertisers' cookies turned off, please visit www.networkadvertising.org. Please note this does not opt you out of being served advertising. You will continue to receive generic ads.

Please understand that Barnes & Noble does not control these third party cookies, and you should check the privacy policy of the Internet advertising company or advertiser to see whether and how it uses cookies.

Whenever you click on links and banners on any Barnes & Noble Website that take you to a third party website, you will be subject to the third party's privacy policies, not Barnes & Noble's. This Privacy Policy applies solely to information collected by the Barnes & Noble enterprise.

In addition, our website includes links to other websites whose privacy practices may differ from those of Barnes & Noble. If you submit personal information to any of those sites, your information is governed by their privacy policies. We encourage you to carefully read the privacy policy of any website you visit.

Safe Harbor

Barnes & Noble's privacy policy has been reviewed by TRUSTe for

transparency, accountability and choice for our collection and use of your personal information. If you have questions or complaints regarding our privacy policy or practices, please contact us at privacy@barnesandnoble.com. If you are not satisfied with our response you can contact TRUSTe here.

Barnes & Noble complies with the U.S. - E.U. Safe Harbor framework and the U.S. - Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from, respectively, European Union member countries and Switzerland. Barnesandnoble.com LLC has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view Barnes & Noble's certification, please visit http://www.export.gov/safeharbor/

Terms of Use

Any dispute between you and us regarding the privacy of your personal information is subject to this Privacy Policy and the terms of use or terms of service applicable to our product or service you use, including limitation on damages, resolution of disputes, and application of the law of the State of New York.

Contact Information

The address for Barnes & Noble is 122 Fifth Avenue, New York, NY 10011. The address for NOOK Media is 76 Ninth Avenue, New York, NY 10011

III. LOWES.COM

Lowe's respects your concerns about privacy. This Privacy Statement applies to personal information we collect on Lowes.com and other official Lowe's sites (including mobile sites) that link to this Privacy Statement, the Lowe's Career Website hosted on brassring.com, official Lowe's survey forms and sweepstakes entry forms on third-party sites and applications that link to this Privacy Statement, official Lowe's mobile applications that link to this Privacy Statement (the "Mobile Applications"), and from use of the in-store Wi-Fi network (the "Store Wi-Fi") (collectively, the "Site"). The credit-related areas of the Site are covered by different privacy notices that appear on the credit application pages or that you receive in connection with your credit accounts, as applicable; the term "Site" does not refer to these areas.

The term "Site" also does not refer to the Weekly Ads pages at lowes.shoplocal.com, the Iris Smart Home website www.irissmarthome.com or the login page for that website on Lowes.com. In some cases, a website or online service covered by this Privacy Statement may provide additional detail about privacy practices specific to the website or online service.

This Privacy Statement describes the types of personal information we collect on the Site, how we may use that information and with whom we may share it. The Privacy Statement also describes the measures we take to protect the security of the personal information. We also tell you how you can reach us to ask us to update your preferences regarding how we communicate with you or answer any questions you may have about our privacy practices.

INFORMATION WE COLLECT

You may choose to provide us with personal information (such as name, contact details and payment information), such as:

Contact information, such as your name, address, telephone number, and email address, and your title or occupation.
Login and access credentials (such as username and password) for Lowe's accounts.
Payment information, such as your payment card number and expiration date.
Date of birth.
The geolocation of your device (such as if you opt to use the "Find Near Me" feature of the mobile-optimized portion of our websites or our Mobile Applications).
The unique ID number associated with certain Lowe's accounts.
Certain information about your Lowe's purchases returns or exchanges.
Personal information in communications and other content you submit, such as photographs, product information and details about your projects and property.
Social media IDs, such as for Facebook or Twitter
Personal information you submit in your capacity as an independent contractor of Lowe's, such as gender, ethnicity and identification numbers such as your NRDS ID number.
Personal information you submit in connection with a job application on the Career Website, such as your name, contact information, Social Security Number, date of birth, employment status, employment history, education information, references, rÃ©sumÃ©, immigration status and ability to work

legally in the United States, driver license information, personal or family employment affiliation with Lowe's, criminal record, and, on a voluntary basis for our Equal Employment Opportunity compliance purposes for jobs located in the US, gender, race and ethnic background.
Back to Top

INFORMATION WE COLLECT BY AUTOMATED MEANS

When you use our Site, we may collect certain information by automated means, using technologies such as cookies, Web server logs, Web beacons and JavaScript.

Cookies are files that websites send to your computer or other Internet-connected device to uniquely identify your browser or to store information or settings on your device. Our Site may use HTTP cookies, HTML5 cookies, Flash cookies and other types of local storage (such as browser-based or plugin-based local storage). Your browser may tell you how to be notified when you receive certain types of cookies and how to restrict or disable certain cookies. You also may be able to delete your Flash cookies or adjust your Flash cookie settings by visiting the Adobe Flash Website Storage Settings Panel and Global Storage Settings Panel. Please note, however, that without cookies you may not be able to use all of the features of our Site or other websites and online services.

In conjunction with the gathering of information through cookies, our Web servers may log information such as your device type, operating system type, browser type, domain, and other system settings, as well as the language your system uses and the country and time zone where your device is located. The Web server logs also may record information such as the address of the Web page that referred you to our Site and the IP address of the device you use to connect to the Internet. They also may log information about your interaction with this Site, such as which pages you visit. To control which Web servers collect information by automated means, we may place tags on our Web pages called "Web beacons," which are small files that link Web pages to particular Web servers and their cookies. We also may send instructions to your device using JavaScript or other computer languages to gather the sorts of information described above and other details your interactions with the Site.

We may use third-party Web analytics services on our Site, such as those of Google Analytics. These service providers use the technology described above to help us analyze how users use the Site. The information collected by

the technology (including your IP address) will be disclosed to these service providers, who use the information to evaluate your use of the Site. To learn about opting out of Google Analytics, please click here.

We may use the information collected through automated means to provide a better tailored shopping experience and for market research, data analytics and system administration purposes, such as to determine whether you've visited us before or are new to the Site, and for compliance with our legal obligations, policies and procedures. We also may use this information to target custom content and ads to you on this and other websites, including as described in the Interest-Based Advertising section below.

Back to Top

INFORMATION COLLECTED AUTOMATICALLY BY THE MOBILE APPLICATIONS

If you elect to install the Mobile Applications, the information we collect may include the following:

Your geographic location, including within a Lowe's store and the surrounding area.
Information about your use of the Mobile Applications.
The type of device you use and its operating system.
Identification details of your device (e.g., unique device identifier).
IP address.
Your use of mobile coupons in a Lowe's transaction.
This information will allow push notifications and other targeted marketing designed specifically for your shopping preferences such as special offers based upon areas in which you may be shopping in the store, and shopping lists with specific items located for your convenience when you are shopping a particular store, as well as for other in-store mapping and routing services. It also may be used for the other purposes specified in this Privacy Statement.

Back to Top

INFORMATION COLLECTED AUTOMATICALLY BY STORE WI-FI

If you elect to use the free Store Wi-Fi available at Lowe's stores, we will collect information such as the following:

The URLs and content of the pages you visit on any website (e.g., on

yahoo.com or Lowes.com) using your mobile device, and, on some websites, information you submit through online forms.
The apps on your mobile device that use the Store Wi-Fi.
Your geographic locations within a Lowe's store and the surrounding area within the range of the Store Wi-Fi.
How long you use the Store Wi-Fi at particular locations.
The type of device you use and its operating system.
Identification details of your device (e.g., unique device identifier and MAC address).
Browser information and IP address.
The address of the store where you use the Store Wi-Fi.
This information will allow targeted marketing designed specifically for your shopping preferences such as specific coupons based upon the sites and pages you visited, special offers based upon areas in which you may be shopping in the store, including competitive offers based upon other websites that you may be viewing, shopping lists with specific items located for your convenience when you are shopping a particular store, as well as for other in-store mapping and routing services. It also may be used for the other purposes specified in this Privacy Statement.

Back to Top

INTEREST-BASED ADVERTISING

Data about your activities online is being collected on our Site for use in providing advertising tailored to your individual interests. You may choose whether or not to have your information collected for that purpose. This section of the Privacy Statement provides details and explains how to exercise that choice.

You may see certain ads on other websites because we participate in advertising networks administered by third parties. These networks track your online activities over time by collecting information through automated means, including through the use of the technologies described in the Information We Collect By Automated Means section above, and they use this information to show you advertisements that are tailored to your individual interests. The information they collect includes information about your visits to our Site, such as the pages you have viewed. This collection and ad targeting takes place both on our Site and on third-party websites that participate in the ad network, such as sites that feature advertisements delivered by the ad network. This process also helps us track the effectiveness of our marketing efforts.

To learn more about ad networks, including how to opt out, click here.

Back to Top

HOW WE USE THE INFORMATION WE COLLECT

We may use the information we collect through the Site to:

Provide, administer and communicate with you about products, services, events and promotions (including by sending you newsletters, coupons and other marketing communications).
Process, record and track your purchases, payments and rebates.
Process, evaluate and respond to your requests, inquiries and applications.
Manage our customer information databases.
Operate registrations, including on MyLowe's and Lowes.com.
Administer contests, sweepstakes and surveys.
Create, administer and communicate with you about your accounts.
Customize your experience with our Site.
Provide you with in-store navigation and mapping services.
Allow you to find locations near you.
With respect to personal information we collect through our Career Website, evaluate your application for employment and contact you regarding possible employment.
Operate, evaluate and improve our business (including developing new products and services; managing our communications; performing market research, data analytics and data appends; determining and managing the effectiveness of our advertising and marketing; analyzing our products, services and Site; administering our Site; and performing accounting, auditing, billing, reconciliation and collection activities).
Protect against and prevent fraud, unauthorized transactions, claims and other liabilities, and manage risk exposure and quality.
Comply with and enforce applicable legal requirements, industry standards and our policies and terms, such as our Terms and Conditions of Use.
We also may use the information in other ways for which we provide notice at the time of the collection.

Back to Top

SHARING OF INFORMATION

We may share personal information we collect on the Site with certain

service providers, some of whom may use the information for their own purposes. For example, (i) our websites may feature live chat functionality, and the information gathered in the chat feature may be collected by or shared with a provider such as LivePerson, whose privacy policies are available at www.liveperson.com/policies/privacy, (ii) information you submit on our Site in connection with a product review may be collected by or shared with a product review company such as Bazaarvoice, whose privacy policy is at www.bazaarvoice.com/privacy-policy and who may publish the information in locations not affiliated with Lowe's, such as the website of the manufacturer of the product you review, and (iii) information submitted on our Careers Website is collected by or shared with the Careers Website provider, Kenexa, whose Privacy Policy is at www.kenexa.com/privacypolicy. We also may share your information among our affiliates, joint marketing partners and companies that fulfill orders placed with us, who may send you marketing information. In addition, we may share personal information we collect on the Site at your request.

We may disclose information about you (i) if we are required to do so by law, regulation or legal process, such as a court order or subpoena; (ii) in response to requests by government agencies, such as law enforcement authorities; or (iii) when we believe disclosure is necessary or appropriate to prevent physical, financial or other harm, injury or loss; (iv) in connection with an investigation of suspected or actual unlawful activity; or (v) to assist in collecting debt owed by you.

We reserve the right to transfer personal information we have about you in the event we sell or transfer all or a portion of our business or assets (including, without limitation, in the event of a reorganization, dissolution or liquidation). Should such a sale or transfer occur, we will use reasonable efforts to direct the transferee to use personal information you have provided to us in a manner that is consistent with our Privacy Statement.

Back to Top

YOUR CHOICES

Where applicable, you may amend your preferences regarding how we communicate with you by updating your profile within your Lowe's authenticated account, using the settings pages on certain websites or contacting us as described in the How to Contact Us section below.

To be removed from all of Lowe's official email, telephone and postal mail

marketing, choose one of the following options: email customercare@lowes.com and type "REMOVE FROM ALL MARKETING" in the subject line; call 1-800-44-LOWES; or send your request by mail to:

Lowe's Customer Care â€“ CON8
P.O. Box 1111
North Wilkesboro, NC 28659

For any of these options, please include your name, address, phone number and email address in the request, and let us know how you provided us with the information.

Back to Top

ACCOUNT PROFILE AND COMMUNICATIONS PREFERENCES GENERALLY

You may access the profile page of certain accounts you maintain on our Site to modify certain personal information associated with your profile and indicate certain communications preferences.

Back to Top

EMAIL

Where applicable, you may amend your preferences regarding how we communicate with you through email by clicking on the "unsubscribe" link in an email you receive from us, by updating certain subscriptions within certain Lowe's authenticated accounts, within settings pages or by contacting us as described in the How to Contact Us section below. To stop receiving newsletters from Lowes.com, you also may email customercare@lowes.com with the phrase "REMOVE FROM NEWSLETTER LIST" in the subject line, and we will apply your preference to the email address from which you send us the request.

Back to Top

INTEREST-BASED ADVERTISING

To exercise your preferences regarding the collection of data for targeted advertising, please follow the directions in the Interest-Based Advertising section above.

Back to Top

STORE WI-FI

To stop the collection of information via Store Wi-Fi, disconnect from the Store Wi-Fi network. Please note that disconnecting from the Store Wi-Fi network will not prevent you from taking advantage of our Mobile Applications' collection of your location. To deactivate that collection of information, follow the instructions in the Mobile Applications section below.

Back to Top

MOBILE APPLICATIONS

To stop collection of information by the Mobile Applications, delete the applications from your device. To stop only the collection of information from the geolocation services available on your device (such as your device's GPS functionality), use your device's settings to deactivate the Mobile Applications' access to those services. Please note that deactivating this access will not prevent you from taking advantage of our Store Wi-Fi's collection of your location. To deactivate that collection of information, follow the instructions in the Store Wi-Fi section above.

Back to Top

THE LOWE'S PRIVACY AND SECURITY STATEMENT

To exercise a choice under a prior version of this statement, contact us as described in the How to Contact Us section below.

Back to Top

NOTICE TO CALIFORNIA CUSTOMERS

Subject to certain limitations under California Civil Code Â§ 1798.83, if you are a California resident, you may ask us to provide you with (i) a list of certain categories of personal information that we have disclosed to certain third parties for their direct marketing purposes during the immediately preceding calendar year and (ii) the identity of certain third parties that received personal information from us for their direct marketing purposes

during that calendar year. To make such a request, please contact us as follows:

Lowe's Customer Care

Attn: Privacy Team â€“ California Marketing Choices â€“ CON8

P.O. Box 1111

North Wilkesboro, NC 28656

1-800-445-6937

Back to Top

HOW WE PROTECT PERSONAL INFORMATION

We maintain administrative, technical and physical safeguards to protect the personal information you provide on our Site against accidental, unlawful or unauthorized destruction, loss, alteration, access, disclosure or use and other unlawful forms of processing.

Back to Top

LINKS TO OTHER WEBSITES

This Site contains links to other websites for your convenience and information. These websites may be operated by companies not affiliated with us. Linked websites, including those operated by Lowe's, may have their own privacy notices, which we strongly suggest you review if you visit them. We are not responsible for the content of any websites that we do not control, any use of those websites or the privacy practices of those websites.

Back to Top

UPDATES TO OUR PRIVACY STATEMENT

This Privacy Statement may be updated periodically and without prior notice to you to reflect changes in our personal information practices or relevant laws. We will post a notice on Lowes.com and certain other parts of the Site to notify you of any significant changes to our Privacy Statement and indicate at the top of the Privacy Statement when it was updated.

Back to Top

BBB ONLINE

We participate in the Council of Better Business Bureau's BBBOnLine program. Further information about this program and its dispute resolution process is available at the Better Business Bureau's website.

Back to Top

HOW TO CONTACT US

If you have any questions or comments about this Privacy Statement, or if you would like us to update information we have about you or your preferences, please contact us as indicated below. When you contact us about personal information we hold about you, please let us know where you provided us with the information.

Lowe's Customer Care
Attn: Privacy Team â€“ CON8

P.O. Box 1111

North Wilkesboro, NC 28656

1-800-445-6937

customercare@lowes.com

IV. OVERSTOCK.COM

Overstock.com Privacy and Security Policy

Overstock.com, Inc. (â€œOverstock.com,â€☐ â€œOverstock,â€☐ â€œwe,â€☐ â€œus,â€☐ or â€œourâ€☐ as appropriate) has created the following Privacy and Security Policy (â€œPrivacy Policyâ€☐) to inform you of the following: what information we collect, when we collect it, how and why we collect it, how we use it, how we protect it, how we share it and what choices you have regarding our collection and use of this information.

This Privacy Policy applies to the following sites: http://www.overstock.com, http://www.o.info, and http://www.o.biz (collectively and individually, the â€œSitesâ€□). Entering the Sites constitutes your acceptance and agreement to the terms contained in this Privacy Policy. If you do not agree with the terms set forth in this Privacy Policy, please do not enter the Sites.

WHAT INFORMATION WE COLLECT

Types of Information We Collect
Your name
Your billing and delivery address
Your e-mail address
Your phone (or mobile) number
Your credit/debit card number
Information on how you are using the Sites
Your purchase/return/exchange information

We Collect Information When
You purchase, order, return, exchange or request information about our products and services from the Sites or mobile applications.
You create an Overstock.com account
You connect with Overstock.com regarding customer service via our customer service center, or on social media platforms.
You visit the Sites or participate in interactive features of the Sites or mobile applications.
You use a social media service, for example, Overstock.com's Facebook page or YouTube channel.
You sign up for e-mails, mobile messages, or social media notifications from Overstock.com.
You enter a contest or sweepstakes, respond to one of our surveys, or participate in a focus group.
You provide us with comments, suggestions, or other input
You interact with any of the Sites through your computer, tablet or mobile device

HOW AND WHY WE COLLECT THE INFORMATION

Technologies Used
We may use tracking pixels/web beacons, cookies and or other technologies

to receive and store certain types of information. This information includes Internet Protocol (IP) addresses, browser information, Internet Service Provider (ISP), operating system, date/time stamp and clickstream data. This information helps us customize your website experience and make our marketing messages more relevant. It also allows us to provide features such as storage of items in your cart between visits. This includes Overstock.com content presented on other websites or mobile applications. In order to provide the best customer experience possible, we also use this information for reporting and analysis purposes, such as how you are shopping our website, performance of our marketing efforts, and your response to those marketing efforts.

Third Party Cookies

We allow third-party companies to collect anonymous information when you visit the Sites and to use that information to serve ads for Overstock.com products or services or for products or services of other companies when you visit the Sites or other websites. These companies may use anonymous information (e.g., navigational, non-personally identifiable information, click stream information, browser type, time and date, subject of advertisements clicked or scrolled over, etc.) during your visits to the Sites and other websites in order to provide advertisements about our goods and services likely to be of interest to you. These parties may use a cookie or a third party web beacon, or other technologies, to collect this information.

To opt out of third-party vendors' cookies, see the â€œWhat Choices Do You Have?â€□ section of this privacy policy for instruction how to do so.

User Experience Information

In order to improve customer online shopping experience, help with fraud identification, and to assist our customer care representatives in resolving issues customers may experience in completing online purchases, we use tools to monitor certain user experience information, including, but not limited to, login information, IP address, data regarding pages visited, specific actions taken on pages visited (e.g., information entered during checkout process), and browser information.

Information from Other Sources

We may also obtain information from companies that can enhance our existing customer information to improve the accuracy and add to the information we have about our customers (e.g., adding address information). This may improve our ability to contact you and improve the relevancy of our marketing by providing better product recommendations or special offers that we think will interest you.

Public Forums

Any information you submit in a public forum (e.g., a blog, chat room, or

social network) can be read, collected, or used by us and other participants, and could be used to personalize your experience. You are responsible for the information you choose to submit in these instances.

Mobile Privacy

Overstock.com offers mobile applications (commonly known as "apps") that allow you to shop online, check product availability, learn about sales events, or receive other information from Overstock. All information collected by Overstock.com via our mobile application is protected by this Privacy Policy. Although you do not have to provide your location information to Overstock.com to use our mobile applications, our services require a zip code to function. If you have questions about location and notification privacy, please contact your mobile service provider or the manufacturer of you device to learn how to adjust your settings.

HOW WE USE THE INFORMATION WE COLLECT

Product and Service Fulfillment

Fulfill and manage purchases, orders, payments, returns/exchanges, or requests for information, or to otherwise serve you

Provide any requested services

Administer sweepstakes and contests

Marketing Purposes

Deliver coupons, mobile coupons, newsletters, receipt messages, e-mails, and mobile messages

Send marketing communications and other information regarding products, services and promotions

Administer promotions

Internal Operations

Improve the effectiveness of the Sites, mobile experience, and marketing efforts

Conduct research and analysis, including focus groups and surveys

Perform other business activities as needed, or as described elsewhere in this policy

Fraud Prevention

To prevent fraudulent transactions, monitor against theft and otherwise protect our customers and our business

Legal Compliance

To assist law enforcement and respond to subpoenas

HOW WE PROTECT THE INFORMATION WE COLLECT

Security Methods

We maintain technical, administrative, physical, electronic and procedural safeguards to protect the confidentiality and security of information transmitted to us. To guard this information, the Sites use Secure Sockets Layer (SSL). SSL encrypts your credit card number, name and address so only Overstock.com is able to decode the information.

E-mail Security

Please note that e-mail is not encrypted and is not considered to be a secure means of transmitting credit card information. "Phishing" is a scam designed to steal your information. If you receive an e-mail that looks like it is from us asking you for certain information, do not respond. Though we might ask you your name, we will never request your password, credit card information or other information through e-mail.

Information About Children

We recognize the particular importance of protecting privacy where children are involved. We are committed to protecting children's privacy and we comply fully with the Children's Online Privacy Protection Act (COPPA). Overstock.com will never knowingly request or collect personal information from any person under 13 years of age without prior verifiable parental consent. If we become aware that an individual is under the age of 13 and has submitted any information to Overstock.com, for any purpose without prior verifiable parental consent, we will delete his or her information from our files.

Additional Security

We also ask customers to carefully review their accounts and immediately report any unexpected activity to Overstock.com and their issuing bank or credit card company. We are asking all our customers to take measures to help protect information in their online accounts, including the following:

Install the latest security updates and anti-virus software on your computer to help prevent malware and viruses

Reset your e-mail account passwords frequently

Use complex passwords (a minimum of 7 alpha/numeric cAsE sEnsitive characters)

Do not use the same password on more than one website

Do not share your password with others

Sign out/log off website sessions so that your session is closed and cannot be accessed by another user on the same computer, especially when using a public computer or terminal

HOW WE SHARE THE INFORMATION WE COLLECT

General Policy

We do not sell or rent customer information to third parties; except, under

limited circumstances outlined below, we may share information with third parties.

The Overstock Family

We share information we collect within the Sites and Overstock.com family, which includes all Overstock.com subsidiaries and affiliates. The Overstock.com family may use this information to offer you products and services that may be of interest to you.

Service Providers

We may share information with companies that provide support services to us (such as a printer, e-mail, mobile marketing, or data enhancement provider) or that help us market our products and services. These companies may need information about you in order to perform their functions. These companies are not authorized to use the information we share with them for any other purpose.

Legal Requirements

We may disclose information you provide to us when we believe disclosure is appropriate to comply with the law; to enforce or apply applicable terms and conditions and other agreements; or to protect the rights, property or safety of our company, our customers or others.

When You Direct Us

At your direction or request, we may share your information.

Business Transfers

If some or all of our business assets are sold or transferred, we generally would transfer the corresponding information regarding our customers. We also may retain a copy of that customer information.

WHAT CHOICES DO YOU HAVE

E-mail

Promotional E-mail

If you do not wish to receive promotional e-mails from us, click here. You also have the ability to unsubscribe to promotional e-mails via the opt-out link included in each e-mail. It may take up to 10 business days before you stop receiving promotional e-mails.

Important Notices and Transactional E-mail

From time to time, we may send non-commercial electronic email messages with important information about us or the Sites to your email address. We regularly send email order confirmations and email order updates to you after you have submitted an order.

Mobile

We may distribute mobile coupons and text messages to mobile devices of customers who have requested this information via an opt-in request.

Customers will be able to opt out of a specific mobile messaging campaign.
Overstock.com Cookies
The help function of your browser should contain instructions to set your computer to accept all cookies, to notify you when a cookie is issued, or to not receive cookies at any time. If you set your computer to not receive cookies at any time, certain personalized services cannot be provided to you, and accordingly, you may not be able to take full advantage of all of the Overstock.com features.
Third Party Cookies
To opt-out of third-party vendor's cookies on other websites, visit the Network Advertising Initiative website, click here http://www.networkadvertising.org/choices/.
Telephone
If you do not wish to receive promotional communication from us, call us at (800) 843-2446 to opt out. This opt out does not apply to operational communication, for example, confirmation of delivery address.

HOW DO YOU ACCESS AND UPDATE THE INFORMATION

In order to keep your information accurate and complete, you can access or update some of your information in the following ways:
If you have created an Overstock.com account, you can log in and update your account information, including contact, billing, and shipping information.
o Contact us with your current contact information and the information you would like to access. We will provide you the information requested if reasonably available, or will describe more fully the types of information we typically collect.

OVERSTOCK PRIVACY POLICY SCOPE

This privacy policy applies to all current or former customer information collected by or provided to Overstock.
The Sites may offer links to other sites. If you visit one of these sites, you may want to review the privacy policy on that site. In addition, you may have visited our website through a link or a banner advertisement on another site. In such cases, the site you linked from may collect information from people who click on the banner or link. You may want to refer to the privacy policies on those sites to see how they collect and use this information.

INTERNATIONAL CUSTOMER PRIVACY

In some cases, Overstock.com has partnered with companies [e.g., FiftyOne, Inc., who does business under the name â€œFiftyOne,â€□ and PayPal, Inc. (â€œPayPalâ€□), collectively, â€œVendorsâ€□] as outside vendors that we have selected to help us facilitate international transactions. We work closely with these Vendors to ensure that your transaction is handled with care and all the information you provide is secure.

As an international customer, when you click on the checkout button, you will be redirected to a checkout page hosted by FiftyOne to complete your order. On the checkout page, you will be required to select a method of payment and submit credit card and other information to FiftyOne to complete your order. On the checkout page, you will be presented with FiftyOne's terms and conditions which you must agree to in order to complete your order.

Upon completion and approval of your order by FiftyOne, FiftyOne will notify us of the approval and we will process your order and cause it to be shipped directly to FiftyOne. In this process, FiftyOne will purchase those items in your order from us, thereby taking title to the items, bill your credit card, collect and remit any duties and taxes to the appropriate taxing authority and arrange for the delivery of your order. In this process, FiftyOne makes the sale to you as the merchant of record, but we are legally obligated to deliver your order as set forth in our Terms and Conditions.

If you have questions about your order, you should direct them to us and not to FiftyOne.

The Vendors may give you the opportunity to receive marketing messages from them, in which case you should refer to their terms and conditions for details about how they use your information.

The Vendors have assured us that they will process information received from you with at least the same level of privacy protection as set forth in the US-EU Safe Harbor Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of information from European Union member countries and Switzerland. If you choose to provide us and/or the Vendors with information, you consent to the transfer and storage of that information on servers located in the United States.

Any information you provide us is controlled and processed by Overstock.com, Inc., 6350 South 3000 East, Salt Lake City, Utah 84121, USA or its suppliers (where indicated herein). As mentioned herein, your information provided at checkout will be controlled and processed a Vendor. Overstock.com complies with the US-EU Safe Harbor Framework and the US-Swiss Safe Harbor Framework as established by the U.S. Department of

Commerce and approved by the European Commission and the Swiss Federal Data Protection Authority. We conduct an annual self-assessment to verify that we are in compliance with the Safe Harbor Privacy Principles in addition to our own Overstock privacy program assessments. Overstock.com has certified to the U.S. Department of Commerce and the European Union that our processing of personal data is in compliance with the Safe Harbor Privacy Principles. For more information about the Safe Harbor program, and to view our certification page, visit the Department of Commerce's Safe Harbor website. While the Safe Harbor Principles are designed to protect information originating in the European Economic area and Switzerland, our policy is to protect all international customer information in accordance with these Principles.

Customers shipping internationally who wish to inquire about or update information or change marketing preferences or anyone who wants to receive information about our international privacy program should contact us directly using one of the following methods:

Send an e-mail to customercare@overstock.com

Call our customer care line at (801) 947-3100

Write us at Overstock, 6350 South 3000 East, Salt Lake City, UT 84121, USA

In compliance with the US-EU and US-Swiss Safe Harbor Principles, Overstock.com commits to resolve complaints about your privacy and our collection or use of your information. European Union or Swiss citizens with inquiries or complaints regarding this privacy policy should first contact Overstock.com using one of the following methods:

Send an e-mail to customercare@overstock.com

Call our customer care line at (801) 947-3100

Write us at Overstock, 6350 South 3000 East, Salt Lake City, UT 84121, USA

Overstock.com has further committed to refer unresolved privacy complaints under the US-EU and US-Swiss Safe Harbor Principles to an independent dispute resolution mechanism, the BBB EU SAFE HARBOR, operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgement of your complaint, or if your complaint is not satisfactorily addressed by Overstock.com, please visit the BBB EU SAFE HARBOR web site at http://www.bbb.org/us/safe-harbor-complaints for more information and to file a complaint.

OVERSTOCK PRIVACY POLICY REVISIONS

By interacting with Overstock, you consent to our use of information that is collected or submitted as described in this privacy policy. We may change or

add to this privacy policy, so we encourage you to review it periodically.

This Privacy Policy was last updated on January 9, 2013.

V. WASHINGTONPOST.COM

At the same time that The Washington Post Company and washingtonpost.com are committed to bringing you information tailored to your individual needs, we recognize the importance of protecting the privacy of your personally identifiable information. In adopting this privacy policy, our intent is to balance our legitimate business interests in collecting and using personally identifiable information and your reasonable expectations of privacy. Please note: this policy applies only to information collected by washingtonpost.com online, as specified below, and does not govern or apply to information collected or used by The Washington Post Company or its affiliates through other means

WHAT PERSONALLY IDENTIFIABLE INFORMATION DO I PROVIDE TO WASHINGTONPOST.COM?

Washingtonpost.com asks you to provide various types of personally identifiable information to enhance your experience on our site. During registration, washingtonpost.com asks for information such as your name, e-mail address, year of birth, gender, Zip code, country, street address, Job Title, Primary Responsibility, Job Industry and Company Size. The more information you provide, the better we are able to customize your experience. We may also ask you for other information at other times - such as when you enter a contest or participate in a promotion, when you post an online ad, when you participate in our message boards, or when you order products from us. Whenever you provide personally identifiable information to us, we will make an effort to link to our privacy policy. See below about â€œcookiesâ€☐ and what other information is collected.

HOW DOES WASHINGTONPOST.COM USE MY PERSONALLY IDENTIFIABLE INFORMATION?

Our primary goal in collecting personally identifiable information is to provide you, the user, with a customized experience on our network of sites. This includes personalization services, interactive communications, online shopping and many other types of services, most of which are completely free to you.

Washingtonpost.com uses the personally identifiable information you provide to us in several ways. Some examples follow.

A user's personally identifiable information may be used by washingtonpost.com for editorial purposes such as to contact you as part of an online survey. Additionally, we may also use the information provided by you to: 1) contact you with legal notices, 2) to advise you of any changes or additions to our Service or terms and conditions, and 3) account status (including confirmation of registrations). If you do not wish to receive the foregoing and therefore unregister from the site, please contact Customer Care and ask to have your registration account deleted. Once your account has been deleted, you will no longer have access to washingtonpost.com, however, you may reregister at any time.

We may also use information about our users and their activities on our site to send offers and information about The Washington Post Company and its affiliates. However, if you no longer wish to receive the foregoing, please contact Customer Care to request removal from this list.

Further, if you told us in your account preferences that you would be interested in receiving certain e-mail newsletters from us, we will send you those e-mail subscriptions. Please note that regardless of those subscription preferences, we may contact you by e-mail as described elsewhere in this privacy policy (e.g., to notify you about changes or additions to our Service, such as new features). However, if you no longer wish to receive any of the foregoing, you may change your preferences for the future at any time by clicking on the following link:
https://ssl.washingtonpost.com/actmgmt/registration/addnewsletter/long

In order to provide services free of charge, we display advertisements. washingtonpost.com delivers targeted advertisements on behalf of advertisers. Advertisers give us an advertisement and tell us the type of audience they want to reach (for example, females over 25 years old). We take the advertisement and display it to users meeting those criteria. In this process, the advertiser never has access to you washingtonpost.com account.

Washingtonpost.com also does research on our users' demographics, interests and behavior based on the information you provide to us including upon registration, on order forms, during a promotion, as well as from our server log files or from surveys. We do this to better understand and serve our users. This research is compiled and analyzed and washingtonpost.com

may share aggregated versions of this data with advertisers or other businesses. In addition, under confidentiality agreements, washingtonpost.com may match user information with third party data.

DO OTHER COMPANIES OR PEOPLE HAVE ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION I PROVIDE TO WASHINGTONPOST.COM?

When you are on an area of washingtonpost.com and are asked for personally identifiable information, you are providing that information to The Washington Post Company, its divisions or affiliates, or vendors providing contractual services for washingtonpost.com (such as hosting vendors and list managers). If personally identifiable information is being provided to and/or maintained by any company other than these, our policy is that we will not transfer that personally identifiable information unless notice is given prior to transfer. If you do not want your information to be shared, you can choose not to allow the transfer by not using that particular service or by expressing this preference, if requested. Additional information about personally identifiable information follows.

Promotions: Promotions that run on washingtonpost.com may be sponsored by companies other than washingtonpost.com or may be co-sponsored by washingtonpost.com and another company. Some or all personally identifiable information provided by you during a promotion may be shared with the sponsor. If information will be shared, we will disclose such sharing prior to the transfer. You can decide not to participate in the promotion if you don't want your personally identifiable information to be shared. In certain circumstances, you may not be able to participate in a particular promotion if you chose not to share personally identifiable information. Currently, most washingtonpost.com promotions are limited to U.S. or North American residents.

Advertisers and Links: washingtonpost.com advertisers, or Web sites that have links on our site, may also collect personally identifiable information directly from you. The information practices of companies collecting data on our site or Web sites linked to washingtonpost.com are not covered by this privacy statement.

Marketplace: If you make a purchase or request a service from a business in Marketplace, the information you provide for that transaction (as well as tracking information and cookies as described below) is provided directly to the Marketplace business. Businesses listed in washingtonpost.com Marketplace have separate privacy and data collection practices.

washingtonpost.com has no responsibility or liability for these independent policies. For more information regarding the business and its privacy policy, go to that business' home page and click on the appropriate link.

Other: If we run competitions or contests on the site, you may be required to provide additional information such as your telephone number and address in order to participate. The exact rules may vary in each case but the specific rules for any contest will state how that information may be used. If you told us in your account preferences that you would be interested in receiving e-mail from us, we may send you e-mails about washingtonpost.com products, promotions, or services as well as on behalf of other companies. You can change your account preferences at any time. In addition, in each advertising email you will be provided an ability to opt-out of receiving future emails from the advertiser.

We do not control the privacy policies of our advertisers, sponsors or other sites or businesses to which we provide hyperlinks or access. Please visit the sites of these businesses to review their privacy policies.

Washingtonpost.com users should also be aware that, when you voluntarily disclose personal information in chat areas or bulletin boards, that information may be collected by others and may result in unsolicited messages from others.

Except as stated in this privacy policy or at the time of collection, a user's personally identifiable information will not be transferred to a party outside The Washington Post Company, its divisions or affiliates, or its service vendors unless notice is given at the time of collection or prior to transfer. washingtonpost.com may also disclose account information in special cases when we have reason to believe that disclosing this information may be necessary to identify, contact or bring legal action against someone who may be violating our User Agreement, may be causing injury to or interference with (either intentionally or unintentionally) washingtonpost.com's rights or property, other washingtonpost.com users, or anyone else that could be harmed by such activities, pursuant to a request from law enforcement, a subpoena, or a court order, or when otherwise may be required by law.

Data Security: We have in place physical, electronic and managerial procedures to protect the information we collect online. However, as effective as these measures are, no security system is impenetrable. We

cannot guarantee the security of our database, nor can we guarantee that the information you supply will not be intercepted while being transmitted to us over the internet.

WHAT INFORMATION DO WEB SERVERS COLLECT?

Web servers serving washingtonpost.com automatically collect certain non-personally identifiable information, such as which pages each user visits and the domain name of visitors. This information is used for various purposes including internal review, to tailor information to individual visitors and other users, for traffic audits, and as described elsewhere in this privacy policy. We also provide this information (as well as information from third-party market researchers) about our users on an aggregated, anonymous basis to our advertisers.

WHAT ARE COOKIES AND HOW DOES WASHINGTONPOST.COM USE THEM?

Washingtonpost.com places a â€œcookieâ€□ on the browser of a washingtonpost.com user's computer to store and sometimes track information about you. A cookie can be used to tell when your computer has contacted a Web site; we may also use the information for editorial purposes and for other purposes such as measuring certain traffic patterns. For example, cookies are used to ensure that you don't see the same ad too many times in a single session and that you do not have to reenter your login name or password during your visit. We may also use cookies to understand your use of the Service. Advertising service vendors that serve ads into our site may also use their own cookies. You may opt out of those cookies as described below. You may opt-out of the cookies delivered by washingtonpost.com by changing the setting on your browser. Please be aware that this will disable all cookies delivered to your browser, not just the ones delivered by washingtonpost.com.

HOW CAN I OPT OUT OF ONLINE ADVERTISING COOKIES?

Online advertising for washingtonpost.com is delivered by the vendor DoubleClick. DoubleClick places cookies on your browser to facilitate serving particular ads â€“ for instance, to help determine whether you have seen a particular advertisement before, to tailor ads to you if you have visited our site before, and to avoid sending you duplicate advertisements. You can opt out of DoubleClick's use of cookies for these purposes by visiting http://www.google.com/intl/en/privacy/.

In some cases, we and advertisers on washingtonpost.com and other sites work with other third-party vendors to help deliver advertisements tailored to your interests. These vendors include ad networks and audience segment providers, and they place cookies on your browser to collect information about your online activity (e.g., the sites and pages you have visited) in order to help advertisers deliver particular ads on our site and other sites that they believe you would find most relevant. You can opt out of those vendors' use of cookies to tailor advertising to you by visiting http://www.aboutads.info/.

Often our advertisers contract with a third-party service to host their ads. In this case, an ad serving vendor contacts the advertisers' hosting service for a particular advertisement. In that case, an independent cookie may be used by the third-party service. We do not have a mechanism to allow visitors to opt-out of cookies from vendors with whom we do not have a contractual relationship.

Kids under 13: Do not send any information about yourself to us - including information like your name, address or e-mail address. In general, we do not knowingly collect personally identifiable information from children under 13. If, in limited circumstances, we do knowingly collect personally identifiable information from a child under the age of 13, we will do so only with verified parental consent prior to collection. In the event that we learn that we have collected any personal information from a child under the age of 13 without verification of parental consent, we will delete that information from our database as quickly as possible.

Technology on the Internet is developing at a rapid pace, and we need to maintain our flexibility in the online arena. If we need to change our policy in the future, we will post these changes as soon as they go into effect.

VI. WUNDERGROUND.COM

PRIVACY STATEMENT

REVISED AS OF OCTOBER 30, 2013 â€" About Our Privacy Statement

The Weather Underground, LLC ("Weather Underground") is strongly committed to protecting your privacy. This Privacy Policy discloses how we

collect, use and share information we gather about you on the Services and the choices you have regarding our use of and your ability to correct the information. "Services" include Weather Underground's wunderground.com Â® website, wxquickie.com, weatherquicke.com, wundermap.com (the "Sites"), and other Internet enabled or wireless means by which Weather Underground provides content to you or receives content from you, including, without limitation, downloadable software applications (including Desktop Gadget and Dashboard Widget desktop applications), mobile web sites, mobile downloadable applications including WunderRadio, content and blog submission services, chat rooms, SMS messaging, and delivery of Weather Underground and WunderRadio content to you at your request.) "Services" also includes alert products. We hope that this disclosure will enhance your experience and reinforce the trust that you place in Weather Underground's products and services.

INFORMATION COLLECTED BY US WITHIN THE SERVICES

In order to maximize your experience and to provide you with enhanced products and services, Weather Underground may collect personally identifiable information ("PII") from you including your name, e-mail address, address, and phone number. For example, we collect PII when you become a member, sign up your weather station or webcam or weather radio, sign up for email or text alerts, sign up for our API (weather information for use on certain platforms), the Weather Desktop Gadget desktop application. Other examples of when we collect personally identifiable information are when you:

Complete a survey
Register for a promotion, contest or sweepstakes
Send us an e-mail message or complete an inquiry form to receive additional information
Submit a photo to WunderPhoto
Report your weather conditions
Participate in an online forum or community,
Request tweets from us, or
Customize the Services.

We also may collect certain information through automated means, such as:

Specific geographic location where you are currently located
Information about your device and device capabilities
Information about your device operating system

Information about the applications on your device
Information about how you use the Services
Your activities on the Services
IP address
Device identifier
Carrier
Browser Type
Browser Identifier
Referring URL

Chat Sessions, Blogs, and Submissions In the case of participation in a chat session, we require that you use the handle you selected when you registered. Please be aware that chat sessions are recorded and may be monitored. Any information including personally identifiable information, that you submit during a chat session, in blog comments, in community discussions, in any other user comment field, or in connection with your content submissions, including photo submissions, can be read, collected, or used by others who access them, and could be used by other users to send you unsolicited messages. We are not responsible for the information, including personally identifiable information, you choose to submit in these forums.

Content Submissions. If you upload or rate photos in WunderPhoto or blog comments, you have to be registered and logged into this feature, and you will be required to provide us with a handle and email address. If you provide us with content, including, without limitation, submissions to WunderPhoto and user comments, any metadata, including, without limitation, geo-location and tags, in that content will become publicly available.

Location Information. In certain instances in our Services, you will be able to input specific location information in order for us to bring up the weather for that location. For that Service, we will ask you to input specific location such as address, city and state. latitude and longitude, country, neighborhood name, beach location, or zip code.

To offer you certain Services, provide advertisements based on your physical geographic location, and engage in the other uses described below, on some devices we provide you the option to opt-in to allow us to use your physical geographic location using GPS, cellular network location based services on your device, or browser services. You may at any time opt-out from these geo-location services by going to the settings on your mobile device.

If you have the WunderRadio mobile application installed on your Microsoft Windows 7 device, you may also opt-out from geo-location by going to the "Settings" menu in the application and toggling location services off. Toggling location services off may also disable certain services in the application.

Alerts and notifications. In certain of our Services, you have the ability to receive push notifications for weather related updates. To provide these services, we may need to collect your email address, phone number, device information, and mobile carrier information, in addition to the zip code or geographic area to which the alert, update or notification pertains. If you no longer wish to receive these types of notifications you may opt-out by turning them off within the settings of your mobile device or the particular Service for which you registered.

HOW WE USE AND SHARE YOUR INFORMATION

One of the most valuable assets of our business is you. Except as described below, Weather Underground does not rent, sell or share personally identifiable information about you with other people or nonaffiliated companies.

A. Weather Underground and its Affiliates

We use information collected on the Services, and disclose information to third parties, including your physical geographic location, to help fulfill your requests or in connection with the operation of the Services, for example to service your account, conduct a transaction or provide a service that you have requested, display information and advertisements that we believe match your interests and profile, facilitate updates to the Services, provide support, notify you if you've won a contest or sweepstakes, improve the working of the Services, and compile statistics about our users and your use of the Services. We and such third parties may on occasion combine information about you with information obtained from other parties to market to you products or services that may be of interest to you. If you sign up for communications from Weather Underground, they may also contain offers from third parties.

At various points, we may provide you with the opportunity to opt in to receive special offers from Weather Underground and its affiliates. If you choose to opt in, Weather Underground and its affiliates will use your personally identifiable information to inform you of other products or

services available from Weather Underground and its affiliates, including The Weather Channel, LLC, WSI Corporation and Weather Central, LP. These products may include, for example, schedules for special programs on The Weather Channel cable network or offers to purchase a calendar from The Weather Channel.

B. Companies Offering Promotions, Products, or Services

At times we will provide you with the opportunity to opt-in to receive promotions, products or services from third party sponsors. With your permission, Weather Underground will periodically send to you, via e-mail, offers and promotions from our third party sponsors which we select based upon your interests or user profile. In this case we do not share your information with the third party sponsors-we do the mailing for them. You will always have the opportunity to opt- out of receiving future offers by following the unsubscribe link included with each email. In other instances, we provide you with the opportunity to receive products and services directly from specifically identified third parties through the Services. In these instances, you must explicitly consent to receive each offer. When you explicitly agree to receive offers from specific third parties, your information is shared with the specific third party to enable them to provide you with the offer you have requested. We are not responsible for the information collection practices of these third parties, and all information provided is governed by the privacy policies of these third parties. You should review the privacy policies of these parties before supplying personally identifiable information to them.

C. Third-Party Processors

When your information is collected on the Services, it may be collected directly by or shared with a selected third parties in connection with the operation of the Services or the provision of services to you ("Third Party Processors"). These Third Party Processors may include, for example, companies that operate our online WunderStore, that process credit card information or handle shipping for Weather Underground, that deliver materials to you via e-mail or postal service, that organize, administer, process, or provide advertising services, and/ or that analyze data on our behalf to help us provide more relevant offers to you and to eliminate the delivery of duplicate offers as well as correcting and/or updating users' data based on information we provide them. We also provide your information to third party mapping service providers to provide you map content for the

Services. Third party processors are authorized to use your information that we provide to them only to carry out the service they are providing for Weather Underground. We require that the third party processors securely store the personally identifiable information we provide to them and maintain it so that it can be accessed when needed for future purposes, and all such Third Party Processors are contractually bound by us to keep the personally identifiable information confidential.

D. Other Web Sites, Other Services, and Links

Like many Web sites on the Internet and other Internet-based services, many of our Services link to pages located on Web sites or services maintained by various other entities. In some cases you may link to pages of other Web sites that are framed with elements of our Services such as in the header or footer. In that case the URL will identify the site you are visiting. In other cases, such as advertisements, you will be connecting to another site or service when you click on or otherwise activate those opportunities, including click-to-call, click-to-text, and click-to-email opportunities. These other sites and services are not bound by our privacy policy, and we are not responsible for their information collection practices. The privacy policies of other organizations may differ from ours, for example, with respect to the level of security, use of cookies, and collection, use and disclosure of personally identifiable information.

Some of our Services allow users to interface with other sites or services, including Facebook and Twitter. You will remain logged in to those other sites and services until you log off those sites and services. By proceeding with these interfaces, you are allowing our Services to access your information on those other sites and services, and you are agreeing to those other sites' and services' Terms of Use. Once you log into those other sites and services, the content you post on those other sites and services may also post to our Services. Your use of those other sites and services is subject to the privacy policies of those sites and services, and not this Privacy Policy.

Some of our Services use third party operating systems, platforms, communication services, devices, and software elements (such as mobile device operating systems, wireless services, mobile phone and tablet devices), and some of our Services are provided by third party distributors, device makers, device operators, platform operators, and communication services. Weather Underground does not control these third party entities, products and services, and they may collect, use, process, transmit and disclose your

information. For example, these third party elements may gather information from our Services, including our applications, in a manner that overrides your settings and preferences in our Services. As Weather Underground does not control or have knowledge of their data handling practices, we recommend that you review their privacy notices, terms of use and license agreements.

E. Use by us of IP Addresses, Cookies, Web Beacons, Single-pixel Gifs, and Information Saved by Other Technologies

Weather Underground and Third Party Processors acting on our behalf use various Internet technologies which help us to manage the operations of our Services and track usage behavior so that we can tailor information and advertisements to make your visits more enjoyable and meaningful. These Internet technologies include:

IP Addresses: numbers assigned to individual computers which accompany every packet of information across the Internet.
Cookies: small electronic files transferred from our services to your electronic device.
Beacons and single-pixel Gifs: electronic tags.
HTML5 LocalStorage: storage within your browser on your electronic device.

Information that Weather Underground collects via the technologies described in this section may be linked to other information about you. Weather Underground uses the technologies described in this section, alone or in combination, to provide and administer our services, understand user behavior, manage services operations, measure the effectiveness of advertisements and our service operations, target advertising, help diagnose problems, recognize repeat visitors, track and analyze usage behavior, facilitate your access to and use of our services, serve, target, control, and measure advertisements on our Services, count users who have visited certain areas of our Services we wish to track, and help determine the effectiveness of advertising campaigns on our services. In addition, we may share demographic information, location data, IP address, aggregate (not individual) usage statistics for our Services, other identifiers and information with advertisers and other third parties. For example, we may share IP address, random or anonymous device identifier, city and state, ZIP code, and specific geo-location with the parties identified in subparagraph F below.

Your browser may allow you to manage your cookies and HTLM5 LocalStorage. Each browser is a little different, so look at your browser Help menu to learn the correct way to modify your cookies and HTML5 LocalStorage. If you turn Cookies or HTML5 Local Storage off, however, you won't have access to many of the features which make your experience more efficient and some of our Services will not function properly.

Weather Underground contracts with certain Third Party Processors to track, analyze and report data about the usage of our Services using these Internet technologies. These Third Party Processors include Google Analytics, Paypal, and Omniture.

F. Use of Cookie, Web Beacon and Other Technologies by Advertisers, Ad Networks, Ad Servers and Analytics Companies

Weather Underground works with a variety of advertisers, advertising networks, advertising servers, and analytics companies. These advertisers, advertising networks, advertising servers, and analytics companies use various technologies, and technologies from third party companies, to collect data in order to send (or serve) relevant ads to users. These technologies may include the placement of cookies or web beacons, the use of HTML5 LocalStorage, the use of unique or non-unique non-personal identifiers, or the use of other technologies on our Services, and these technologies may be used to track user behavior, to track how our Services are being used, and possibly to serve you more relevant ads. These targeted advertisements may appear on our Services or other services that you visit. This Privacy policy does not cover the use of various technologies by advertisers, advertising networks, advertising servers, and analytics companies. These companies may also obtain information from services you use from other companies, including without limitation, other websites, mobile website, mobile downloadable applications, and downloadable applications, and combine that information with information they obtain through these third party technologies on our Services. You should be aware that The Weather Underground does not have control over these third party technologies or the information contained in them. For more information about how DoubleClick, and some of the other ad networks, ad servers, analytics companies, and third party companies use the information collected by the technologies on our services and about your option not to accept cookies placed by some of these companies on our Services, please visit the following sites:
DoubleClick: http://doubleclick.net/privacy_pilocy,

Nielsen: http://www.nielsen-netratings.com/privacy/sitecensus.htm
Quantcast: https://www.quantcast.com/how-we-do-it/consumer-choice/privacy-policy/
Flurry: http://www.flurry.com/privacy-policy.html
Google Analytics: http://www.google.com/analytics/learn/privacy.html
Omniture: http://www.omniture.com/static/61
comScore and its affiliate, Scorecard Research:
http://www.scorecardresearch.com/Priv.html
http://networkadvertising.org/managing/opt_out.asp
and http://www.aboutads.info/choices

These opt-outs are device specific and may not work on all devices. You should be aware that if you choose to opt out through any of these sites, this does not opt you out of being served advertising. The ads will just not be targeted to you by any party from which you have opted out.

You can also opt out of future information collection from our Services by ceasing use of the Service or in the case of an application, uninstalling the application.

G. Purchase or Sale of Businesses

Weather Underground continually looks for ways to improve our business, including purchasing or selling all or part of a business or company. If we buy or sell a business, personally identifiable information and non-personal information will likely be transferred as part of the sale. If we buy a business, we will honor the requests of that business' former customers regarding their personally identifiable information. If in connection with a sale there will be material changes to the way personally identifiable information is being used, affected consumers who have provided us with an email address will be notified via e-mail, if you have provided us an email address, and will be given the opportunity to opt-out.

H. Other Limitations on Privacy

We may provide personally identifiable information without your permission (i) pursuant to judicial or other government subpoenas, warrants, or orders or otherwise to comply with law; (ii) where The Weather Underground believes the rights, property or an individual's safety or security is at risk; iii) if we find that your actions violate our Terms and Conditions of Use; or iv) where otherwise required by law.

E-MAIL A FRIEND

If you choose to use our service that allows you to e-mail parts of our Services to a friend, in most circumstances we need to have access to your and your friend's e- mail addresses temporarily to send the e-mail due to technical requirements. This information is not used for any other purpose.

MOBILE DEVICE CONTACTS

Some mobile products allow you to view weather conditions for people in your phone's contact list. If you agree to use this feature, your contact list will be accessed in order for us to provide weather information for your contacts who already have their address, city, state, or zip code available. We do not store this information or use it for any other purpose.

OPTING-OUT, CORRECTIONS AND CANCELLATIONS

If you receive an offer or promotion from Weather Underground or a third party related to Weather Underground, you must have opted in. To ensure we have your consent, we make sure that each e-mail sent to you by Weather Underground presents the additional opportunity to opt-out of receiving future e-mails.

If you have registered with us and have obtained a password, you may reset your password, update your personally identifiable information, correct information, make changes to your preferences, unsubscribe to any e-mail subscriptions or opt-out of certain services, by accessing your profile online at the member settings page or within the settings of a particular application or you may contact us directly at wuhelp@wunderground.com.

DATA RETENTION OF ACCOUNT INFORMATION

If you wish to cancel your account or request that we delete or no longer use your account information to provide you Services, contact us at wuhelp@wunderground.com. Subject to applicable law, we will retain and use your account information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

CHILDREN'S PRIVACY

Weather Underground is committed to protecting the safety and privacy of young people using the Internet. We do not knowingly collect personally identifiable information from children under the age of 13 and believe that children should get their parents' or guardians' consent before giving out any personally identifiable information.

The Services may contain links to third party Web sites and other services geared to children. The linked sites and services are not under the control of Weather Underground. We are not responsible for the contents of any linked site or service or any link contained in a linked site or service, nor are we responsible for the privacy practices of the operators of those sites or services with respect to children. We strongly encourage parents and guardians to review the privacy policies of all linked sites and services.

INTERNATIONAL TRANSFER

Weather Underground, and all associated Services and systems, including registration, is housed on servers operated in the United States. If you are located in the European Union or elsewhere outside of the United States, please be aware that information we collect (including cookies) will be processed and stored in the United States, a jurisdiction in which the data protection and privacy laws may not offer the same level of protection as those in the country where you reside or are a citizen. By using our Services and providing information to use, you consent to the transfer to and processing of the information in the United States.

OUR COMMITMENT TO SECURITY

Keeping the information you provide to Weather Underground secure is important to us. We have put in place appropriate physical, electronic and managerial procedures designed to protect and safeguard your data. Of course, although Weather Underground uses standard industry practices to protect your personally identifiable information, we cannot guarantee that your communications with the Services will never be unlawfully intercepted, or that your personally identifiable information will never be unlawfully accessed by third parties.

CHANGES TO THE PRIVACY POLICY

Weather Underground reserves the right to alter our Privacy Policy as business needs require. If we decide to change our Privacy Policy, we will post those changes here so that you will always know what information we gather, how we might use that information and whether we will disclose it to anyone. All changes to this policy will be posted on our Web site prior to the time they take effect. In the event that we make material changes to the way we use personally identifiable information, affected consumers who have provided us with an e-mail address will be notified via e-mail and will be given the opportunity to opt-out.
The Weather Underground, LLC
P.O. Box 724554
Atlanta, GA 31139
DATA FEEDS

If you connect to Wunderground Data Feed, you will be able to pull and to decode weather related data from the non-public website of Weather Underground, Inc. ("WUI").

Your access to Wunderground Data Feed, and your use of the data pulled from Wunderground Data Feed, is subject to the Terms of Use generally applicable to all features of www.wunderground.com. (the "Site")

In addition, because of the special features of Wunderground Data Feed, by accessing and viewing information from Wunderground Data Feed you agree to be bound by these special terms: (1) you will not modify the data from Wunderground Data Feed in any way; (2) you will not modify the link structure to Wunderground Data Feed; (3) you will not modify WUI's logo that is included in the data; and (4) in all uses of the data, you will credit WUI by name as the source of the data.

As with all data that you access from the Site, the data that you pull from Wunderground Data Feed may only be used by you for personal, non-commercial purposes. If you want to use that data for commercial purposes, contact us through the Site and we will supply you with rate information for commercial customers.

If you violate any of the general or specific terms applicable to Wunderground Data Feed, WUI has the right to terminate your use of the Site and the Data Feed and to take appropriate legal actions against you.

WUI reserves the right to change these general or special terms at any time by posting on the Site. You understand and agree that your use of the Site and Wunderground Data Feed is a benefit voluntarily given by WUI and that WUI may withdraw that benefit and rescind your participation at any time for any reason in its sole discretion. If you do not agree to these general and special terms, you cannot use Wunderground Data Feed or the services and information offered therein.