

Privacy Policies: How To Communicate Effectively with Consumers

By Shannon Wheatman and Michelle Ghiselli

iapp



Summary:

This paper discusses the regulatory and judicial consequences to your business of failing to make sufficiently clear, accurate and comprehensible privacy disclosures; reports common problems with privacy policies; highlights findings from a new study evaluating the privacy policies of Fortune 500 companies, and offers tips on how to design an effective and clear privacy policy.

The complete white paper version of this article, **Privacy Policies: How to Effectively Communicate with Consumers and Avoid Judicial and Regulatory Scrutiny** may be found at www.kinsellamedia.com/privacypolicies.pdf.

Introduction

If you conduct business with or on behalf of consumers, then you collect, use and share at least some type of personal information about your customers.

In many cases, customers provide information directly by ordering products, contacting a company, providing information on a company's website, checking a box or taking some similar action. Many companies, though, collect much more information without relying on the customer's input.

Web analytics and ad-related companies track customers' browser software and devices as they move from page to page within a site and, sometimes, across different websites. If your company works with third-party marketers, then your customers' browsing history and purchasing choices are being collected.

There is also a good chance that you are making very specific promises to your customers about how your company collects, uses, shares and discloses information collected online.

How confident are you that those promises are accurate and complete? Further, how certain are you that the promises you are making are being effectively communicated to and received by customers?

According to a [2012 Internet Trend Report](#), 79 percent of the U.S. population is now online. Never before have so many different types of consumers, from all educational levels and socio-economic backgrounds, been online. So, it is critical that companies through their online privacy policies effectively communicate with an audience that encompasses a wide range of the U.S. population.

With a growing trend towards plain language requirements and government-sponsored and government-encouraged best practices for

protecting consumer privacy, companies not only must be proactive about communicating their privacy practices, but also holistic in their approach to information governance.

The Legal Push for Plain Language

The U.S. has historically depended on industry and companies to self-regulate online privacy practices and disclosures. In recent years, however, it has begun to explore ways to motivate companies to increase self-regulation, improve privacy practices and disclosures and enforce violations. Furthermore, the class action plaintiffs' bar has also targeted dozens of companies for allegedly deficient privacy disclosures.

The Federal Trade Commission (FTC)

- Preliminary Staff Report: "[Protecting Consumer Privacy in an Era of Rapid Change](#)"

» The FTC found that most corporate privacy policies are "incomprehensible," stating that, generally speaking, "privacy policies do a poor job of informing consumers about companies' data practices or disclosing changes to their practices."

- Multiple settlements have:

» Stressed the importance of clear privacy policy disclosures and found non-adherence to be a deceptive trade practice in violation of [Section 5](#) of The Federal Trade Commission Act of 1914.

» Signaled that the FTC would closely review and interpret actual privacy policy wording, particularly in the areas of information use/sharing and how changes to the policy will be handled.

The Department of Congress (DOC)

- The DOC stressed the need for a plain language approach to drafting privacy policies in its [Privacy Green Paper](#), identifying "transparency" as a top priority in promoting privacy.
- In February 2012, the DOC unveiled "[Consumer Data Privacy in a Networked World](#)," stating "[p]lain language statements about personal data collection, use, disclosure, and retention help consumers understand the terms surrounding commercial interactions."

"Informing just isn't informing
when no one reads it—
especially if you know no one reads it."
—*San Francisco Chronicle*

State of California

Sen. Ellen Corbett introduced the [Social Networking Privacy Act](#) (SB 242), which would require social media websites to explain privacy settings in "plain language."

Amended the [data breach notification](#) bill to require that consumer data breach notification letters be written in plain language. This requirement is the first of its kind among state breach notification laws.

The Need for Plain Language Policies

[Studies have shown](#) that consumers do not understand their options when it comes to their privacy—meaning they may not believe that they can limit how companies' use their personal information.

To read a dense, legalistic and highly technical privacy policy, an individual must not only be educated, but also must possess the time and motivation required to wade through a sea of technical and legal jargon. Therefore, most consumers remain uninformed about the way a company collects, uses and discloses their information because, in most cases, privacy policies are the only source of information about a company's privacy practices and the consumers' options in managing their personal information.

How **easy** is your company's privacy policy to find and does it have a **prominent** place on your website?

Three major problems with current privacy policies are:

- 1) The incomprehensibility of the language and/or structure of privacy policies;
- 2) The “cost” of reading privacy policies (and small likelihood of them being read in any meaningful way), and
- 3) The elements of privacy policies that make them less useful as decision-making tools.

Plain language privacy policies provide clear and effective communication of complex and important information to people with basic education. Clear writing and effective presentation can help promote consumer understanding which saves a company time and money.

A [Georgia Institute of Technology \(GIT\) study](#) agrees, noting that “in general, websites

did poorly on notification for notifying users of changes to their policies,” a finding which negated the concepts of transparency and informed consent.

When dealing with online content targeted at children, the Children's Online Privacy Protection Act and the FTC's implementing rule require websites and interactive mobile apps to provide notice and obtain parental consent before collecting personal information from children under age 13. Ensuring that parents know and understand your company's privacy policy and are, therefore, providing informed consent is key.

A new study evaluating the privacy policies of Fortune 500 companies offers tips on how to design an effective and clear privacy policy.

Fortune 500 Privacy Policy Study

To determine whether online privacy policies are clear, Dr. Shannon Wheatman and Michelle Ghiselli, the authors of the study, reviewed the privacy policies of the [Fortune 500 companies](#). The sample included 454 online privacy policies—46 did not have online privacy policies.

A readability analysis was conducted on each privacy policy using the Flesch-Kincaid readability test, the most widely used readability scale. This measure of readability indicates the number of years of education that a person needs to be able to understand the text easily on the first reading; a score of 12 means the text would be understood by a high school graduate, a score greater than 12 means the text can be understood by someone with a college education. In general, this test penalizes for multi-syllable words and long,

complex sentences. The authors also reviewed the location of the privacy policy on each company’s website to determine whether the policy would be conspicuous to consumers.

User-Friendliness

Most privacy policies in our study were “[user-unfriendly](#)” because they were very difficult to locate on company websites. If a privacy policy is not made prominent on a company’s website it will be overlooked by consumers. Even if the privacy policy is written in plain language, if it cannot be readily found, it is useless.

The link to most of the Fortune 500 privacy policies were inconspicuous with over 95 percent providing a link to the privacy policy at the bottom of the homepage in a small font. [Research has shown](#) that a hard-to-read font is likely to cause consumers to not act; *i.e.*, not read.

Readability

The [2010 U.S. Census](#) found that 13.3 percent of the U.S. population over the age of 18 has less than a high school education, and only 27.8 percent has a bachelor’s degree or higher. Most importantly, people read a few grade levels below their highest level of educational attainment and the [average U.S. adult reads](#) at an eighth-grade reading level. Therefore, your company’s privacy policy will not be understood if it is written at a higher reading level than that possessed by your customers.

A clear majority of the privacy policies in the Fortune 500 Study were written at a level that surpasses the reading ability of the average U.S. adult (see Fig. 1). In fact, more than 82 percent of the Fortune 500 privacy policies required a

college reading level. The table below shows the reading level of the privacy policies in the study and also presents the percentage of the U.S. population who has attained that level of education.

Grade Level	Fortune 500 Privacy Policies	Percent of U.S. Adults
Less than High School	40 (8.8%)	91.3%
High School	41 (9%)	86.7%
College	330 (72.7%)	27.8%
Post-Graduate	43 (9.5%)	9.6%

Figure 1

Difficulty

In order to understand the average privacy policy in the study at least two years of college education are needed, grade level 14.11. This dovetails with the GIT Study, which found an average grade level of 14.21. The lowest reading level in the Fortune 500 Study was 8th grade, the average reading level of the U.S. adult and only one privacy policy met it. The highest grade level was 26, or 10 years of post-graduate work.

Length

Most of the privacy policies would require the average reader more than seven minutes to read, using 250 words per minute as a benchmark. The average privacy policy was 1,660 words long—around six and a half minutes—and the wordiest was 7,718 words long, taking on average 31 minutes to read.

Taking into consideration that the [average amount of time](#) a person spends on a

website is 42 seconds, consumers are unlikely to spend seven minutes reading a privacy policy, let alone 31.

Clarity

From a communications perspective, the language used in many privacy policies is deficient. The majority of privacy policies in the study do not follow accepted standards for effectively written communication.

Most use complicated, legalistic words and phrases that consumers are not likely to understand, instead of clear, simple terms and references and do not often explain concepts that are foreign to the average consumer. [Research](#) has shown that “[t]he use of legalese [or technical language] within contracts often creates difficulties for consumers when they try to understand what contractual provisions obligate them to do, allow them to do, or forbid them from doing.” Writers should assume that privacy policies will be read by a variety of consumers who shop, buy, work and live their lives without needing a detailed understanding of cookies, aggregated or anonymized data, personally identifiable information (PII), geolocation data, P3P, etc.

Writing a Plain Language Privacy Policy

A full discussion of tips for writing a plain language privacy policy can be found in Kinsella Media’s [Plain Language Primer for Privacy Policies](#).

Choose your words

When writers choose their words, they need to focus on common equivalents of legal and technical jargon—a style that may be antithetical to your company’s legal or IT

departments. However, the idea that clear, transparent language would make a privacy policy *less* precise is wrong. Much like legal documents, using plain language in your company’s privacy policy clarifies vague or ambiguous concepts and elements—and [can help identify](#) any gaps, errors or deficiencies that more complicated language may hide.

In drafting a privacy policy, your company should think about how you might draft an advertisement. If companies know how to get their point across when selling customers goods and services, privacy authorities will expect them to use those same communications skills in explaining information practices.

Because you have a thorough understanding of your company’s privacy practices, you may be tempted to turn the draft privacy policy into a wholesale data dump. This is where many privacy policies fall apart, weighed down with lengthy recitations and disclaimers that simply do not matter to consumers. This is more than a style problem; it can affect perception of your company’s attitude toward transparency.

Know your audience

Privacy notices can be significantly improved through deliberate changes in language, organizational structure, formatting and presentation of the policy.

In writing privacy policies, the demographics of the users are important, but only to a point. In actuality, the education and comprehension levels of users vary so widely that privacy policies must be written in the simplest conversational English. A reading level of eighth grade is desirable and knowing any

special considerations of your audience; e.g., age, etc., is key. Above all, make sure someone other than lawyers can read and understand the communication.

Implementing plain language

Focus on information that consumers need to know to make choices, but may not already know. As much as possible, describe privacy issues in “if this, then that” terms. For example; “*if* you use the website, *then* this is what we will collect. *If* you want to create a registered account *then* this is what we need. *If* you have a question or complaint, *then* contact us here.”

It is important that users understand what information is being collected, what will be done with it and what their choices are.

A consensus exists among plain-language experts about the basic guidelines that make documents easy to understand:

Omit legal/technical jargon and limit defined terms (your privacy policy should not read like a technical manual),

- Use positive language,
- Avoid double negatives,
- [Active voice is less ambiguous](#) than passive voice,
- Pare down sentences to essential thoughts,
- Omit superfluous words,
- Use personal pronouns,
- Question and answer format will personalize the communication.

Designing an Effective Notice

There is more to a privacy notice than just words on a page; the design, layout and placement of a notice also influence readability.

Design the notice using a reader friendly format that will entice consumers to want to take time to review it. Advertisements have seconds to grab the attention of the reader, and research shows headlines are read first.

Use an informative headline to alert the reader that the notice may affect them. Then use simple, descriptive headers to organize the document into manageable sections grouping related information.

Fonts need to be large enough so the average person can easily read the notice. Fonts vary in size, but keeping the text at 12 points or above eases readability. Using Internet-friendly fonts like Verdana or Arial will also help with readability, and remember to keep in mind the size of the screen and the device being used.

If the consumer has to follow a link, make sure the link is easy to find and in a reasonable size font. COPPA requires companies to place such a link in a “clear and prominent place and manner on the home page of the website.” Appropriate spotlighting of key information also breaks up the text and lets readers know what is important.

- Emphasize key points by using bullets, underlining and/or italics
- Never use all CAPITAL LETTERS for sentences or paragraphs—it is the most difficult type to read
- Use highlighting in moderation
- Use examples to describe practices or put the content into an easy-to-read chart

Conclusion

Jon Leibowitz, former chairman of the FTC, [remarked](#), “privacy policies have to get better. They have to get simpler. They have to be

sort of like a nutrition guide on the side of a cereal box so people can really understand.” Companies *cannot* underestimate the difficulty of writing an effective privacy policy and the time that is needed to do it right.

The Fortune 500 Study shows that most privacy policies are poorly written, inconspicuously placed on websites and unlikely to be understood by the average consumer. So, indeed, companies need to do better.

Furthermore, the rate of technological change is increasing, making the task of understanding company practices challenging. Moreover, how cookies, web beacons, pixels and the like are used one day does not tell you how they might be used the next. Unfortunately, [a 2011 study by PriceWaterhouseCoopers](#) revealed “39 percent of nearly 10,000 executives in 138 countries said they reviewed their privacy policies annually,” down from 52 percent in 2009.

Keep in mind that your company will change the technology it uses, its business practices or partners. Even best practices or customer expectations can change. It is time for privacy policies to be in step with the evolution in technology. Privacy policies should anticipate change and be designed and continuously re-designed to effectively communicate changes to consumers.

Addressing policy changes in a forthright manner is critical, but these changes must also be kept up-to-date. If a company’s privacy policy does not reflect its actual privacy practices, there is no informed consent and both sides are at risk.

When changes occur, your company needs to make clear to consumers how you will communicate them, and what will constitute consumers’ consent to revised privacy policies. You may need to get consumers’ affirmative consent to changes that will impact their privacy—accomplishing this requires planning and logistical analysis. Remember, transparency is critical to consumer trust of your brand.

The key take-away from the FTC and DOC reports is that demonstrating good intentions and good faith preventive efforts can work in your company’s favor with regulators; and effectively designing your privacy policy, making it conspicuous on your company’s website and using clear and concise language can help demonstrate that good faith.

Related Research and Publications:

[*Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices*](#), CHI LETTERS, Vol. 6, No. 1, 471, Carlos Jensen & Colin Potts (2004)

[*Protecting Consumer Privacy in an Era of Rapid Change*](#), Federal Trade Commission (2010)

[*Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*](#), U.S. Department of Commerce Internet Policy Task Force (2010)

[*Consumer Data Privacy in a Networked World*](#), U.S. Department of Commerce (2012)

[*Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users*](#), Erica Newland *et al.* (2011)

[*Plain Language Primer for Privacy Policies*](#), Kinsella Media, (2012)

[*The Cost of Reading Privacy Policies*](#), I/S: J. L. POL'Y FOR THE INFO. SOC'Y 1, 2-3, Aleecia M. McDonald & Lorrie Faith Cranor (2008)

[*Why Privacy Policies Don't Work—And What Might*](#), San Francisco Chronicle, James Temple, (January 29, 2012)

[*A Comparative Study of Online Privacy Policies and Formats*](#), Privacy Enhancing Technologies Lecture Notes in Computer Science, Vol. 5672, 37-55, Aleecia M. McDonald *et al.* (2009)

[*Majority of Class Action Publication Notices Fail to Satisfy Rule 23 Requirements*](#), The Review of Litigation, Vol. 30, No. 1, 53, 54-55, Shannon R. Wheatman & Terri R. LeClercq (2011)

[*Short Definition of Plain Language*](#), PLAIN LANGUAGE, Robert Eagleson

[*Answering the Critics of Plain Language*](#), 5 SCRIBES J. LEGAL WRITING 51, 62-65, 73, Joseph Kimble (1996)

[*Making Legal Language Understandable: A Psycholinguistic Study of Jury Instructions*](#), 79 COLUM. L. REV. 1306, Robert Charrow & Veda Charrow (1979)

Readability vs. Comprehensibility: A Case Study in Improving a Real Document, Veda Charrow, in Linguistic Complexity and Text Comprehension: Readability Issues Reconsidered 85 (Alice Davison & Georgia M. Green eds., 1988)

[*Comprehension of Legal Contracts by Non-experts: Effectiveness of Plain Language Redrafting*](#), Michael Masson & Mary Ann Waldron (1994)

[*The Principles of Readability*](#), 1, William H. DuBay (Aug. 25, 2004)

[*Writing for Dollars, Writing to Please: The Case for Plain Language in Business, Government, and Law*](#), 105, Joseph Kimble (2012)

[*Consumers concerned about their online privacy*](#), Consumers Union (Apr. 3, 2012)

[*Evolution of a Prototype Financial Privacy Notice*](#), Kleimann Communication Group, Inc. (2006)

[*Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand*](#), 30 BULL. SCI., TECH. & SOC., no. 2, 2010 at 130, 131, Anca Micheti *et al.* (2010)

[*A License to Deceive: Enforcing Contractual Myths Despite Consumer Psychological Realities*](#), 5 N.Y.U. J. L. & BUS. 617, 656–57, Debra Pogrud Stark & Jessica M. Choplin (2009)

[*If it's Easy to Read, it's Easy to do, Pretty, Good, and True*](#), Hyunjin Song and Norbert Schwarz, 23 THE PSYCHOLOGIST 108, 108 (2010)

[*The Principles of Readability*](#), 1, William H. DuBay (Aug. 25, 2004)

[*Traditional and New Media in Class Action Notice - The State of Play*](#) Alicia Gehring and Maureen Gorman (Spring 2013)

[*Fortifying your defenses: The role of internal audit in assuring data security and privacy*](#), PriceWaterhouse Coopers (2012)