That’s Not Privacy!

We need a revolution in the way we engage people on privacy issues. We are somehow stuck in the 1990s where a privacy policy on a website is supposed to be the way to assure people that we care about privacy. With new technologies and services soon to be generating and collecting vast amounts of information, and analytics able to identify and discern great amounts of information on us, we need to get out of this rut.

In December of 2014, the Pew Research Center released a study revealing that 52 percent of online Americans don’t know what a privacy policy is.¹ A majority of respondents believed that “[w]hen a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users.” In reality it is merely a disclosure of some or all of the ways a company collects, retains, and shares with third parties personally identifiable information (PII). In other words, it’s a list of ways the user’s personal data are not private and not under their control.

At the same time, however, internet users are not entirely naïve: they know their personal information is being collected. Another recent survey found that 91 percent of American adults think “consumers have lost control over how personal information is collected and used by companies.”² So it is clear that while Americans are keenly aware about their lack of real privacy online, they incorrectly believe that so-called “privacy policies” constitute an effort to protect them and their personally identifiable information.

Joseph Turow, professor at the University of Pennsylvania’s Annenberg School for Communication, believes two main factors contribute to the confusion surrounding privacy policies:

1. “Many people don’t actually read privacy policies; they simply look at the label. And the intuitive understanding—the cultural understanding—of the label is that when something says ‘privacy policy,’ it protects your privacy.”³
2. “Privacy policies are often difficult to interpret, even to the small number of consumers who do try to read them.”⁴

There are existing efforts aimed at addressing Turow’s second concern. Most recently, in August, TIME magazine partnered with the Center for Plain Language to “assess, exalt and shame some of the world’s leading tech companies for how they’ve presented privacy information to millions of users,”⁵ and the companies were rated on “how well they follow plain-language guidelines.”⁶ In addition, there have been numerous attempts to develop privacy policy best practices, examples, and templates, all focused on making them more readable and understandable.⁷

But that still leaves the problem of consumers’ mistaken faith in anything labeled a “privacy policy.” We believe the time is ripe to begin a truth-in-labeling initiative. Policies that truly protect privacy are going to become even more important in the future of the Internet of Things, where we don’t necessarily interact with a company and share information through a website but rather through hardware and other services. We may not actually even know what information is being generated by our technologies. It will become even more important for us to help people understand these important issues and companies and governments will have to reconsider how they communicate with

---

³ Smith, Hal of Online Americans quoting Turow (cited in note 1).
⁴ Id.
the public. A first step is to get this old problem fixed. Then we can start having genuine and real conversations about the policies and practices companies and governments need to have to protect our privacy.

The idea
Our idea is simple: we will build a coalition of participating organizations who currently have “privacy policies” on their websites, that will commit to relabeling those policies as either “data usage policies” or (even clearer) “data usage and protection policies” or “how we use your information” all on the same day. In addition, these companies will sign a short statement, written by Civic Hall and Privacy International, explaining their actions. The statements will be collected on a new website, ThatsNotPrivacy.com, to be launched with a press release and conference call that garner attention to the cause.

To be clear, we are not asking companies to change the content of their existing policies. There is a greater debate going on as to what level of privacy is necessary online, now and in the future, what data should be generated and collected, how they should be used, and so on. That conversation is currently limited to the group of security experts, academics, and commercial and government entities that are party to it. Our hope is that this exercise in transparency and truth-in-labeling will help bring a much larger constituency—the public—into the fold. Then we can start asking the institutions we interact with: how are we genuinely protecting privacy, rather than merely articulating some standard text at the bottom of your website?

Legal requirements
Many people with whom we have already spoken have expressed apprehension about the labeling change, and are under the impression that the term “privacy policy” is required by law. However, that is not the case, even under the strictest statutes, those of California and Europe.

California law
The California Online Privacy Protection Act of 2003 (CalOPPA) requires that any “operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California … shall conspicuously post its privacy policy on its Web site.” The law also lists what information must be included in the policy (e.g., the categories of PII the operator collects and third-parties with which it may share the data, etc.). Notably, though, it says nothing about what such a policy need be titled. Indeed, the privacy policy recommendations provided by the Attorney General of California suggest “[mak[ing] the policy recognizable by giving it a descriptive title.”

What the statute does require is that the policy be conspicuously available. Because most websites don’t post their privacy policies on their homepage, they must link to the page wherein it is contained. This can either be done with an image or hypertext, and CalOPPA is clear on what those links must look like.

If the link is an image, it has to contain the word “privacy,” period. If it’s text, however, there’s a little more leeway. In fact, the link must only do one of the of the following:

(A) Include[] the word “privacy.”
(B) [Be] written in capital letters equal to or greater in size than the surrounding text.
(C) [Be] written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the sur-

---

8 Emphasis added—the economic importance of California and the borderless nature of internet commerce extends the range of this statute globally.
9 California Business & Professional Code § 22575(a). For convenience, the Act in its codified entirety is included in Appendix A.
10 Id at § 22575(b).
rounding text of the same size by symbols or other marks that call attention to the language.\textsuperscript{13}

According to the statute, as long as formatting distinguishes the link from surrounding text, or even more broadly, if the link is “so displayed that a reasonable person would notice it,”\textsuperscript{14} it satisfies the conspicuity requirement.\textsuperscript{15}

Finally, in addition to not being statutorily required, the label of “privacy policy” is less within the spirit of the law than “data use policy,” or something in that vein, as the stated purpose of a policy is to notify users of how their data are being collected and used, not to lull them into a false sense of “privacy” protection.

\textsuperscript{13} Id at §§ 22577(b)(3)(A)–(3)(C).
\textsuperscript{14} Id at § 22577(b)(4).
\textsuperscript{15} We concede, and our lawyers agree with her opinion, that the California Attorney General recommends using the word “privacy” in the link \textit{and} making it even more conspicuous with formatting to ensure compliance with the law.
European law

Under European law, everyone has a right to the protection of their personal data, which can only be gathered legally under strict conditions, and for a legitimate purpose.\(^{16}\) However, in addition to being outdated, the 1995 E.U. data protection rules were implemented differently in the 27 member states, so a reform process began in 2012.\(^{17}\) That process is ongoing, so there may be imminent changes to the rules.

As of today, though, the European law says even less than U.S. law about what a purported “privacy notice” must be named. In fact, the description of what information must be given to a “data subject” does not prescribe at all how the information must be presented to him or her, only that the “data controller” must provide the following:

The identity of the controller and of his [or her] representative, the purposes of the processing for which the data are intended, and any further information such as the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, or the existence of the right of access to and the right to rectify the data concerning him [or her].\(^{18}\)

Moreover, the Information Commissioner’s Office in the UK\(^{19}\) calls the “privacy notice” term overly technical, and even suggests titling such a disclosure, required by the UK’s implementation of the 1995 EU rules discussed above, “how we use your information.”\(^{20}\)


\(^{19}\) An independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

\(^{20}\) Information Commissioner’s Office, Privacy notices code of practice at 4 (cited in note 7).
Why should you take part?
Discussion about privacy, especially online privacy, is taking the global center stage. The U.S. and E.U. are engaged in lengthy talks about transmittance of PII across the Atlantic Ocean. Debates about encryption and the mythical “backdoor” grow more fiery every day. The Snowden revelations have brought government snooping to the forefront of public awareness. Yet most people don’t realize what a so-called “privacy policy”—contained on virtually every website—is or does, and one of the reasons for that is simply that the label is misleading.

What they genuinely want to know is how their privacy is being protected, and how they may maintain control of their personal information in modern life.

There’s no reason for keeping the misleading label around. Increased transparency will not only harmonize concerns over real privacy around the world, allowing for increased international commerce, but has also been shown to be a key factor that builds consumer trust in a company.

So, join us for That’s Not Privacy! day! Be transparent about your data usage—show that you care about keeping your customers informed. We want to help you build a long-lasting relationship based on trust.

For this project, we consulted:

Fernando A. Bohorquez, Jr., Partner, Baker & Hostetler LLP
Geff Brown, Assistant General Counsel (privacy, data protection), Microsoft

22 Id at 4.
John Frank, VP & Deputy General Counsel, Microsoft
Maria-Martina Yalamova, Associate, Covington & Burling LLP
APPENDIX A:

CALIFORNIA BUSINESS AND PROFESSIONS CODE §§ 22575–22579

22575. (a) An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site, or in the case of an operator of an online service, make that policy available in accordance with paragraph (5) of subdivision (b) of Section 22577. An operator shall be in violation of this subdivision only if the operator fails to post its policy within 30 days after being notified of noncompliance.

(b) The privacy policy required by subdivision (a) shall do all of the following:

(1) Identify the categories of personally identifiable information that the operator collects through the Web site or online service about individual consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.

(2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process.

(3) Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator’s privacy policy for that Web site or online service.
(4) Identify its effective date.

(5) Disclose how the operator responds to Web browser "do not track" signals or other mechanisms that provide consumers the ability to exercise choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across third-party Web sites or online services, if the operator engages in that collection.

(6) Disclose whether other parties may collect personally identifiable information about an individual consumer's online activities over time and across different Web sites when a consumer uses the operator's Web site or service.

(7) An operator may satisfy the requirement of paragraph (5) by providing a clear and conspicuous hyperlink in the operator's privacy policy to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer that choice.

22576. An operator of a commercial Web site or online service that collects personally identifiable information through the Web site or online service from individual consumers who use or visit the commercial Web site or online service and who reside in California shall be in violation of this section if the operator fails to comply with the provisions of Section 22575 or with the provisions of its posted privacy policy in either of the following ways:

(a) Knowingly and willfully.
(b) Negligently and materially.

22577. For the purposes of this chapter, the following definitions apply:

(a) The term "personally identifiable information" means individually identifiable information about an individual consumer
collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:

1. A first and last name.
2. A home or other physical address, including street name and name of a city or town.
3. An e-mail address.
4. A telephone number.
5. A social security number.
6. Any other identifier that permits the physical or online contacting of a specific individual.
7. Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision.

(b) The term "conspicuously post" with respect to a privacy policy shall include posting the privacy policy through any of the following:

1. A Web page on which the actual privacy policy is posted if the Web page is the homepage or first significant page after entering the Web site.
2. An icon that hyperlinks to a Web page on which the actual privacy policy is posted, if the icon is located on the homepage or the first significant page after entering the Web site, and if the icon contains the word "privacy." The icon shall also use a color that contrasts with the background color of the Web page or is otherwise distinguishable.
3. A text link that hyperlinks to a Web page on which the actual privacy policy is posted, if the text link is located on the homepage or first significant page after entering the Web site, and if the
text link does one of the following:

(A) Includes the word "privacy."

(B) Is written in capital letters equal to or greater in size than the surrounding text.

(C) Is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.

(D) Any other functional hyperlink that is so displayed that a reasonable person would notice it.

(E) In the case of an online service, any other reasonably accessible means of making the privacy policy available for consumers of the online service.

(c) The term "operator" means any person or entity that owns a Web site located on the Internet or an online service that collects and maintains personally identifiable information from a consumer residing in California who uses or visits the Web site or online service if the Web site or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a Web site or online service on the owner’s behalf or by processing information on behalf of the owner.

(d) The term "consumer" means any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes.
22578. It is the intent of the Legislature that this chapter is a matter of statewide concern. This chapter supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the posting of a privacy policy on an Internet Web site.

22579. This chapter shall become operative on July 1, 2004.
APPENDIX B:

VARIOUS EXAMPLES OF CURRENT “PRIVACY POLICY” LAYOUTS

PART I: VARIOUS STYLES

Welcome to the Google Privacy Policy

When you use Google services, you trust us with your information. This Privacy Policy is meant to help you understand what data we collect, why we collect it, and what we do with it. This is important; we hope you will take time to read it carefully. And remember, you can find controls to manage your information and protect your privacy and security at My Account.

Privacy Policy

Data Policy

We give you the power to share as part of our mission to make the world more open and connected. This policy describes what information we collect and how it is used and shared. You can find additional tools and information at Privacy Basics.

As you review our policy, keep in mind that it applies to all Facebook

Your Privacy Matters

At LinkedIn, our fundamental philosophy is “members first.” That value powers all of the decisions we make, including how we gather and respect your personal information.

We’ve crafted the policy below to be as clear and straightforward as possible. Our aim is for you—our members—to always feel informed and empowered with respect to your privacy on LinkedIn. Visit our Safety Center for tips on using LinkedIn smartly and securely.

View our California DNT notice
PART I: VARIOUS STYLES (cont’d)

Privacy Policy

Lyft is dedicated to protecting Your personal information and informing You about how We use it. This privacy policy applies to transactions and activities and data gathered through the Lyft Platform. Please review this privacy policy periodically as We may revise it without notice. This privacy policy was last revised on December 8, 2014. Each time You use the Lyft Platform or provide Us with information, by doing so You are accepting the practices described in this privacy policy at that time.

P&G Privacy Notice

Scope

P&G’s Global Consumer Privacy Policy applies to consumer information, including personal information, collected and used by The Procter & Gamble Company and its affiliated companies and subsidiaries (“P&G”).

To read P&G’s full Global Consumer Privacy Policy click here.

Information P&G Collects

- P&G collects information about you from a variety of sources, including:
  - Information we collect from you directly.
  - Information we collect about you when you call us, visit our sites, use our mobile applications or services, or view our online advertisements.
  - Information we collect about you from other sources, such as commercially available sources.
- All the information P&G collects about you may be combined to improve our communications with you, and to develop world-class products and services.
APPENDIX B (cont’d):

PART II: VARIOUS LENGTHS

Scale is 1:20 (5% of actual size)

Created by the Common Data Project
www.common dataproject.org