BerkeleyLaw
UNIVERSITY OF CALIFORNIA

University of California, Berkeley
School of Law
396 Simon Hall
Berkeley, CA 94720-7200

[Submitted by http://www.ftc.gov/os/publiccomments.shtm]

August 8, 2011

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 2003

Re: Dot Com Disclosures, P114506

Dear Commissioners,

Thank you for taking comments on Dot Com Disclosures.

Q2: What issues raised by new technologies or Internet activities or features on the horizon should be addressed in a revised business guide?

New technologies allow web sites to track individuals in subtle ways, and even to undo consumer-initiated preferences concerning tracking. For instance, we found in 2009 that many popular websites were using Flash Cookies to track individuals online. We also found that some websites were using Flash Cookies to "respawn" user-deleted HTTP cookies.[1] In 2011, using similar methods, we found less Flash cookie respawning. But we did find a popular website using a third-party service that respawned cookies using a different method (cache cookies/ETags).[2] This service was respawning both HTTP cookies and HTML5 local storage.

The revised business guide should make clear that businesses should honor consumers' expressed privacy preferences, and that businesses should not use technical means of any kind to circumvent or otherwise make ineffective consumers' actions taken to protect their privacy. This recommendation is particularly important because of the emergence of server-side unique tracking methods, such as browser

[1] Soltani, Ashkan, Canty, Shannon, Mayo, Quentin, Thomas, Lauren and Hoofnagle, Chris Jay, Flash Cookies and Privacy (August 10, 2009). Available at SSRN: http://ssrn.com/abstract=1446862.
[2] Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan and Hoofnagle, Chris Jay, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning (July 29, 2011). Available at SSRN: http://ssrn.com/abstract=1898390

fingerprinting.[3] As server-side tracking methods are developed, it will become more difficult to determine what websites are doing.

Q5: What research or other information regarding the effectiveness of disclosures – and, in particular, online disclosures – should the staff consider in revising "Dot Com Disclosures"?

A model disclosure approach would prohibit a website from using the term "privacy policy" unless that website's practices comport with common understandings of the protections that privacy policies offer. Specifically, if websites share personal information with third parties, their online disclosure of their practices should not be labeled "privacy policy."

As I argued with colleagues in 2007:

> The large majority of consumers believe that the term "privacy policy" describes a baseline level of information practices that protect their privacy. In short, "privacy," like "free" before it, has taken on a normative meaning in the marketplace. When consumers see the term "privacy policy," they believe that their personal information will be protected in specific ways; in particular, they assume that a website that advertises a privacy policy will not share their personal information. Of course, this is not the case. Privacy policies today come in all different flavors. Some companies make affirmative commitments not to share the personal information of their consumers. In other cases, however, privacy policies simply inform consumers that unless they "opt out" of sharing certain information, the company will communicate their personal information to other commercial entities.
>
> Given that consumers today associate the term "privacy policy" with specific practices that afford a normative level of privacy protection, the use of the term by a website that does not adhere to these baseline practices can mislead consumers to expect privacy that, in reality, does not exist. This is not to suggest that companies intend to mislead consumers, but rather that consumers today associate certain practices with "privacy policy" just as they associate certain terms and conditions with the word "free."

[3] Peter Eckersley, *How unique is your web browser?,* Proceedings of the Privacy Enhancing Technologies Symposium (PETS 2010), Springer Lecture Notes in Computer Science (p. 1-18)(2010), available at http://www.springerlink.com/index/0J1M07443GU00H07.pdf.

> Because the term “privacy policy” has taken on a specific meaning in the marketplace and connotes a particular level of protection to consumers, the Federal Trade Commission (“FTC”) should regulate the use of the term “privacy policy” to ensure that companies using the term deliver a set of protections that meet consumers’ expectations and that the term “privacy policy” does not mislead consumers during marketplace transactions.[4]

Dot Com Disclosures should include a recommendation that businesses that advertise a “privacy policy” provide some baseline privacy protections that meet established consumer expectations.

Many privacy policies use innocuous-sounding terms to mask third-party information sharing. For instance, sites use the terms “affiliate,” “affinity,” “partner,” or “company with products we think will interest you” to mean "we sell your data to third parties with whom we have no operational or ownership interest." The FTC should clarify in the guidance that disclosures should accurately portray information sharing as occurring among true affiliates and third parties. Currently, the consumer cannot distinguish among sites that share with third parties and those that do not.

For instance, the privacy policy on Anntaylor.com reads:

“To respect your privacy, Ann Taylor will not sell or rent the personal information you provide to us online to any third party… In addition, Ann Taylor may share information that our clients provide with specially chosen marketing partners.”

Similarly, what are consumers to make of Smartmoney.com’s privacy policy, which early in the policy claims no third party information sharing but then much later (because of a California law mandate) discloses data sharing to companies, “that sell goods and services that we believe would be of interest”?

"SmartMoney will not sell, share or otherwise disclose any personally identifiable information about our current or former web site users to third party companies or individuals, except as permitted or required by law."

---

[4] Joseph Turow, Chris Hoofnagle, Deirdre K. Mulligan; Nathaniel Good, & Jens Grossklags, *The Federal Trade Commission and Consumer Privacy In the Coming Decade*, 3 I/S J. of Law & Policy 723 (2007).

[…]

"...From time to time we may make our customer lists available to companies that sell goods and services that we believe would be of interest. Customers have the option of having their names and identifying information removed from those lists (subject to certain exceptions and limitations in applicable laws) by contacting us at support@smartmoney.com. We may also from time to time make our customer lists available for direct marketing purposes to other entities that are affiliated with us. If you would like to be removed from those lists, contact us at support@smartmoney.com."

Q6: What specific types of online disclosures, if any, raise unique issues that should be considered separately from general disclosure requirements?

Over the next ten years, the major consumer protection problems with disclosure will surround two popular marketing techniques: the use of "free" and negative option offers. When items or services are marketed as "free", it affects consumers deeply, tempting them with false promises of zero-cost, no-risk transactions. But when free is used as a marketing tool online, there is almost always a true cost hidden in the form of use or sale of personal information.

Figure 1: A "free" offer that claims that privacy isn't the basis of the transaction.

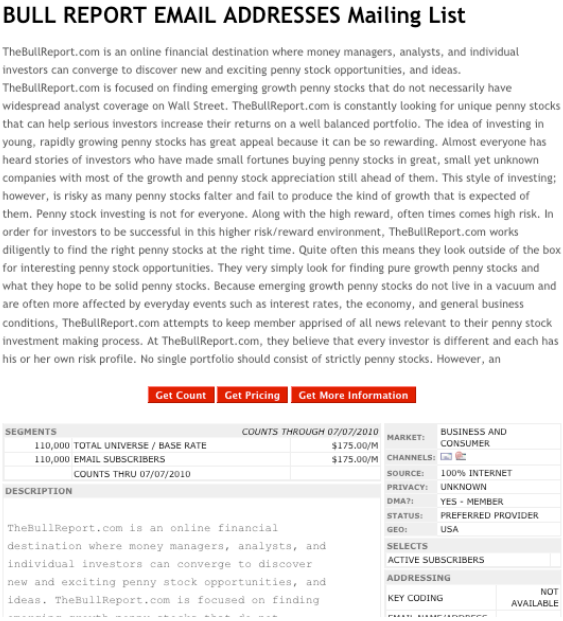

Figure 2: Datacard features "unknown" privacy and DMA membership, and offers two channels for rental.

Model disclosures surrounding free would not bury data use in a privacy policy (for reasons articulated above) but instead the advertisement itself should indicate that use, processing, or sale of personal information is the basis of the bargain.

Consider this: if consumers believe that the mere presence of a privacy policy means that a website cannot sell data, they may rationally conclude that free offers online carry no privacy risk at all. In this mental model, a free offer online may appear to be the same as receiving a sample of food from a restaurant at the mall. But in reality, free offers online are almost always a tactic to collect personal information for some type of reuse. *Dot Com Disclosures should recommend that free offers disclose that personal information is the basis of the bargain in the offer itself.*

Negative options are also going to proliferate, because payment companies have made it exceedingly easy to levy recurring charges upon consumers' credit cards.

Q9: What issues relating to disclosures have arisen from such multi-party selling arrangements in Internet commerce as (1) established online sellers providing a platform for other firms to market and sell their products online, (2) website operators being compensated for referring consumers to other Internet sites that offer products and services, and (3) other affiliate marketing arrangements?

The New York Attorney General's case in Datran Media focused upon an important principle: when buying information for marketing purposes, the buyer should investigate whether the data are being sold consistently with the consumer-facing privacy policy governing the data. Recall that in Datran, the New York Attorney General pursued a marketing company for buying a list of personal information from websites that promised not to sell data.[5]

Data buyer due diligence is important because an astonishing number of datacards on the main market for information sale have an "unknown" privacy status, such as the Bullreport datacard *supra*. In a forthcoming paper, my team analyzes a sample of over 10,000 datacards displayed on lists.nextmark.com, and finds that while over 4,700 claimed to be collected through opt-in methods, just over 6,000 have an "unknown" privacy status.

Of the consumer email lists offered for sale on NextMark, 61.6 percent are provided by Direct Marketing Association (DMA) members (Bullreport card, *supra*, claims to be a DMA member but there is no way to verify this, because the DMA hosts its membership list behind a paywall).

[5] Kevin Newcomb, E-mail Marketer Slapped for Privacy Violations, ClickZ, Mar. 13, 2006, available at http://www.clickz.com/3591116.

DMA members agree to follow certain consumer protection and privacy norms. However, apparent DMA members still sell many lists with unknown privacy status. Over 3,800 data cards offered by DMA members have an "unknown" privacy status, while 2,800 have an "opt-in" privacy status. In fact, we found that DMA membership is significantly and negatively correlated with "opt-in" privacy status, and positively correlated with "unknown" privacy status (chi square=11.992, p=.001). In our sample of over 10,000 data cards, we observed that non-DMA members offered opt-in lists in 46 percent of cases, while DMA members offered opt-in lists almost 43 percent of cases. DMA members offered "unknown" privacy data cards in over 57 percent of cases, while non-members did so in almost 54 percent of cases.

Thus, relying upon DMA membership alone is inadequate to determine the underlying privacy rules governing information sold. *Dot Com Disclosures should explicitly recommend that data buyers investigate the privacy rules governing any information they seek to purchase.*

Q11: What other changes, if any, should be made to "Dot Com Disclosures"?

To aid consumers in determining the policies to which they agreed to, and to assist the FTC in enforcement actions, Dot Com Disclosures should recommend that websites maintain an online archive of both their privacy policies and their Terms of Service.

Respectfully submitted,

/s

Chris Jay Hoofnagle