Submitted by: Daniel Zukerman, Chicago, IL

PRIVACY POLICIES: THE PROBLEM OF MUTABLE TERMS

Others have written at length about the privacy debate surrounding the increasingly common business practice of linking on-line data gathered on the basis of the terms in a Web site's privacy policy to personal information for commercial use; creating and selling individual profiles according to such characteristics as age, occupation, salary, marital status, medical conditions, political affiliations or even as to what kind of toilet paper one prefers to use.[1]

Of course, this brings the inevitable question of "so what?" to the forefront of the debate—like the example my e-commerce law professor would ask all of us—"So what if people know what kind of toilet paper I use—they can put it up on a billboard a top of the Lincoln Tunnel." Notwithstanding, this paper assumes as its starting point that privacy does matter to consumers.

With the presumption that privacy matters to consumers, this paper examines the problem involving the actual capture and use of personal information in transaction-generated situations by Web sites, which frequently occurs on the basis of obliging, non-binding and ambiguous privacy policies due to what I will call "mutable terms." Mutable terms are express statements within a Web site's privacy policy that reserve the right for a Web site to change their privacy policy at any time. Such statements as "we reserve the right to change this privacy policy at our discretion" essentially allows a Web site to change the terms of its privacy policy after consumers have already consented, rendering meaningless any consent given by the consumer on

---

[1] Galil, Yair Y., *No Child's Play: Treatment of Contractually Protected Private Information in Bankruptcy Proceedings*, 2002 Colum. Bus. L. Rev. 823

the basis of the previously agreed upon terms.[2]

Privacy policies are, in effect, displayed to "reassure consumers that their privacy is respected,"[3] informing them about what happens to the personal information they provide by disclosing a Web site's collection and use practices.[4] Though, with that said, the mere posting of a privacy policy does not ensure adequate privacy protection for consumers because often Web sites either violate their own policies or simply don't follow them because of mutable terms,[5] coupled with the lack of effective monitoring and enforcement—which I will discuss later.

However, Web sites that do not explicitly assert the mutability of its privacy policy, i.e. that "the rules may change," regarding their collection and use of information practices, but then later change its terms and apply it retroactively must, in fact, comply with the representations made at the time the personal information was collected or they run the risk of being prosecuted by the FTC due to violating their own privacy policies under Section 5 of the Federal Trade Commission Act (FTCA) for deceptive online information practices.[6]

For example, one particular case prosecuted under Section 5 of the FTCA involved the virtual toy store Toysmart, which sold toys via a website **http://www.toysmart.com.**[7] Toysmart

---

[2] Colloquium on Privacy & Security, Gary M. Schober-Moderator, Shubha Ghosh-Organizer, Ann Bartow, Chris Hoofnagle, Phyllis Borzi-Panelists, Spring / Summer, 2002, 50 Buffalo L. Rev. 703

[3] Larry E. Ribstein, *Law v. Trust,* 81 B.U. L. Rev. 553, 558 (2001)

[4] See Ribstein, supra note 553

[5] Paige Norian, *The Struggle to Keep Personal Data Personal: Attempts to Reform Online Privacy and How Congress should Respond,* 52 Cath. U.L. Rev. 803

[6] See Norian, supra 803

[7] Daniel Bronski, Conway Chen, Matthew Rosenthal and Robert Pluscec, *eCOMMERCE: FTC vs. Toysmart,* 2001 Duke L. & Tech. Rev. 10

collected personal information from its customers including names, addresses, credit card numbers, shopping preferences and family profile data[8] under the following privacy policy: "Personal information voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party. All information obtained by toysmart.com is used only to personalize your experience online. When you register with toysmart.com, you can rest assured that your information will never be shared with a third party."[9]

In addition to its privacy policy, Toysmart exhibited a TRUSTe seal on its Web site, certifying that the personal information customers provided to Toysmart would never be shared with, or sold to, third parties.[10] However, when Toysmart went bankrupt, all those promises inevitably went out the window and the toy company tried to sell its most valuable asset—the consumer personal information.[11]

The FTC sued Toysmart to halt the sale of its customer database, but only after TRUSTe showed it was incapable of preventing Toysmart from selling its customer database on its own.[12] The FTC alleged that Toysmart violated the consumer protection laws and privacy rights of its customers under Section 5 of the FTCA for deceptive online information practices.[13]

---

[8] See Bronski, supra 10

[9] See Bronski, supra 10

[10] See Bronski, supra 10

[11] See Bronski, supra 10

[12] See Bronski, supra 10

[13] See Bronski, supra 10

Ultimately, Disney, who owned fifty percent of Toysmart, bought the consumer personal information for $50,000 and then destroyed it to save both the toy company from having to go to trial and itself from the imminent bad publicity.[14] But what if Disney did not do that? Here, we had a case where consumers relied on the representations made in Toysmart's privacy policy and consented to the terms only to see those same terms violated by the toy company while at the same time discovering just how vulnerable their personal information was in cyberspace.

It is my view that certain provisions need to require Web sites that don't expressly state mutable terms in their privacy polices, but later change those terms when facing bankruptcy, to write their privacy policies in such a particular way that it will restrict consumer personal information—so it is not considered an asset in bankruptcy. Or, the bankruptcy code, itself, should be amended to reflect this concept.

However, what about the privacy policies that expressly state mutable terms? Many of the busiest Web sites have mutable terms in their privacy policies, however, allowing businesses to "change the rules of the game" after consumer consent due to an open-ended policy gives businesses a "free hand to collect personal information without consumers' knowledge or agreement,"[15] which in turn could have a "devastating effect on the public image of an individual"[16] if the information is unreasonably revealed.

Most Web sites now display a privacy policy, and nearly every one of them begin with

---

[14] Shubhankar Dam, *Remedying a Technological Challenge Individual Privacy and Market Efficiency; Issues and Perspectives in the Law Relating to Data Protection*, 15 Alb.L.J.Sci. & Tech. 337

[15] See Dam, supra note 337

[16] See Ribstein, supra note 553

the words "Your privacy is important to us."[17] However, in the U.S., consumers continue to show a "great reluctance to offer their personal information to a Web site because they neither trust, nor are willing to rely on,"[18] the mutability of the promises made in privacy policies.

Following the Toysmart case, consumers' vulnerability was exposed even further when ebay and Amazon.com drew upon the express mutable terms in each of their privacy policies to change their information collection and use practices, notifying consumers that certain protections regarding personal information once promised had now been removed.[19] In effect, ebay and Amazon.com told their customers that if either one of them went bankrupt, they too would sell consumer personal information.

I am concerned with the fact that mutable terms in privacy policies currently allow Web sites like ebay and Amazon.com to sell consumer personal information that they previously assured customers would not be sold. For instance, a Web site should not be allowed to alter an item or detail in its privacy policy after receiving personal information without acquiring consumer consent, i.e. "changing the rules of the game"—even if it explicitly states that it has the right to change its privacy policy at any time.[20]

So how do we solve the mutability problem of privacy policies? One way I propose to solve, or at least limit, the mutability problem would be to require a competent framework of notice and consent regarding a Web site's privacy policy.

---

[17] See Ribstein, supra note 553

[18] See Galil, supra note 823

[19] See Ribstein, supra note 553

[20] See Ribstein, supra note 553

A competent or "beefed-up" and detailed notice requirement, as opposed to the lackluster array of current unregulated and insufficient privacy notices, would be a step in the right direction in enabling consumers the opportunity to understand the mutable nature of privacy policies and its relationship to a Web site's prospective collection and use of information practices prior to its collection. Subsequently, an "actual" consent would permit consumers to then decide whether to provide their personal information to the Web site.[21]

However, under the current U.S. self-regulatory approach, there are no requirements for a Web site to even have a privacy policy let alone a sufficiently disclosed one with a notice detailing its mutability and collection and use of information practices.[22] This raises a number of questions regarding the current state of actual notification consumers receive from the displayed notice on Web sites and whether consumers are properly equipped with the necessary information in hand to be an informed decision-maker capable of providing actual consent.[23]

In order to have a competent notice, privacy policies should explicitly advise consumers of the Web site's information collection and use practices and its subsequent mutability while clearly and intelligibly listing all possible uses of such information.[24] This is because not only are most consumers unaware of the mutable nature of privacy policies and the sheer magnitude of information collected and used by Web sites, but they are particularly unaware of the

---

[21] See Ribstein, supra note 553

[22] Mark E. Budnitz, *Privacy Protection For Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate*, 49 S.C.L. Rev. 847 (Summer 1998)

[23] See Dam, supra note 337

[24] See Dam, supra note 337

consequences such an open-ended policy has on the development of profiles.[25]

Thus, though not perfect, in theory, by closing the privacy policy knowledge gap between Web sites and consumers regarding the collection and use practices of personal information, it should reduce the overall uncertainty involving the automated process of providing personal information as well as the possibility of personal information being collected and used without consumers' knowledge.[26]

However, don't write the obituary for the mutability problem just yet because even if consumers are notified about the mutable nature of a Web site's privacy policy, by its own definition, the mutability makes it very difficult for them to understand how that "effects what information is being collected or what harm might result"[27] because it is nearly "impossible to know where the information will end up and how it will be used and combined with other data"[28]—basically making it a Herculean task for consumers to meaningfully assess the risks associated with providing consent.

There are problems with consent as well because it is directly linked to notice.[29] In fact, for there to be an actual consent, consumers must be able to "choose between different possibilities."[30] Opt-in and opt-out options have bandied about—each giving consumers greater

---

[25] James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U.Colo.L.Rev.1, 26-27 (2005)

[26] See Nehf, supra note 26

[27] See Nehf, supra note 26

[28] See Dam, supra note 337

[29] Paul M. Schwartz, Commentary: *Internet Privacy and the State*, 32 Conn. L. Rev. 815 (Spring 2000)

[30] See Schwartz, supra note 815

control over their personal information.[31] However, despite the opt-in and opt-out options, many times a Web site's privacy policy seems to be more of a "coerced agreement"[32] rather than an informed choice due to the market-based movement of "take-it-or-leave-it processing of consumer information."[33]

Under this take-it-or-leave-it processing, consumers are typically handicapped because information.[34] Subsequent acceptance to the terms, and hence a "consent," is implied from a simple action such as clicking past the Web site's home page.[35]

In effect, this takes choice out of the equation and basically merges notice and consent into one action, essentially permitting notification of a Web site's mutable privacy policy to act as an actual consent to the terms.[36] This is an example in which an "existing practice has become an acceptable standard"[37] and thus has placed consumers in an unenviable position because there is no bargaining.[38] When consumers are faced with this conundrum, standardized terms jumbled

---

[31] See Schwartz, supra note 815

[32] See Schwartz, supra note 815

[33] See Schwartz, supra note 815

[34] See Schwartz, supra note 815

[35] See Schwartz, supra note 815

[36] See Schwartz, supra note 815

[37] See Schwartz, supra note 815

[38] See Schwartz, supra note 815

together in a mutable privacy policy, they often accept them because the only other alternative is to log off from the Internet[39]—this is why consumers won't refuse to deal with Web sites that have mutable approaches to privacy.

For these reasons, it is my view that it is necessary to prohibit the mutability of privacy policies on the Internet. In certain terms, the absence of effective privacy protection prohibiting mutable terms in a Web site's privacy policy exploits consumers by placing consumer personal information in a constant state of fluctuating security without regard to consequences. This, in turn, weakens consumers' confidence in the way personal information is gathered during transaction-generated situations on-line, and thus, undermines the development of the Internet as a secure and viable commercial entity.[40]

The question then becomes who should regulate privacy policies and require such provisions within them? In contrast to the state regulated approach in the E.U., consumer personal information in the U.S. is protected through a hodgepodge of recommended yet voluntary guidelines and private sector self-regulation that indicate the market "may not be willing to agree on privacy safeguards which will adequately protect consumers and provide them with sufficient remedies to cure privacy invasions."[41] In short, under self-regulation, we have little hope in correcting the mutable privacy policy problem because the marketplace will not correct the problem on its own. But why?

Although self-regulation assumes that all privacy problems should be settled by the

---

[39] See Schwartz, supra note 815

[40] See Budnitz, supra note 847

[41] Jay P. Kesan & Andres A. Gallo, *Optimizing Regulation of Electronic Commerce*, 72 U.Cin.L.Rev. 1497 (Summer 2004)

marketplace, Web sites have "no incentive to provide good privacy protection since they can profit from lax rules."[42] Consequently, the self-regulatory approach is skewed toward the collection and use of personal information on the Internet.[43]

When providing personal information on the Internet, consumers must be allowed to know who is collecting and using their personal information,[44] however, in a self-regulatory approach—one that polices itself—it is very difficult to actually know whether Web sites are following the practices stated in their privacy policies.[45]

The absence of an effective monitor permits Web sites to "reap the benefits of using information it collects"[46] without ever "realizing"[47] the consequences for such breaches of one's privacy policy because the misuses usually go undetected. This general ineptness exhibited in the self-regulation of privacy policies as a whole to monitor a given Web site's breach dealing with the collection of consumer personal information is further compacted by the frequent demonstrated lack of authority and subsequent inability for enforcement.[48]

However, privacy policies could be an effective means for gauging compliance, especially if privacy seal organizations, such as TRUSTe and BBBOnline, certify those policies

---

[42] See Kesan, supra note 1497

[43] Jonathan P. Cody, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 Cath.U.L.Rev. 1183 (Summer 1999)

[44] See Cody, supra note 1183

[45] See Cody, supra note 1183

[46] See Cody, supra note 1183

[47] See Cody, supra note 1183

[48] See Ribstein, supra note 553

as veritable through a simple "seal."[49] But with a history of being "toothless in its enforcement against licensees,"[50] like for instance in the Toysmart case, the U.S. may start looking for other alternatives.[51]

It is my view that the Internet requires a regulatory approach in which the FTC and the private sector, perhaps a "tougher" type of seal, work collaboratively to solve privacy issues in ways that are flexible and responsive to the specific characteristics of the Internet while not inadvertently inhibiting technological innovation.

Federal legislation offers uniformity and predictability that would curb the unlawful collection and use of personal information while substantially increasing consumer confidence in online transactions. Of course, the first step for the FTC would be to require a Web site to have a privacy policy. Then, the second step would be for the FTC to require certain provisions in those privacy policies. However, the key to structuring any type of top-down regulation of privacy policies involving consumer consent begins with stopping or at least limiting the mutability of the terms, otherwise consumer personal information rests at the discretion of a business.

Top-down regulation protecting privacy is not new to the U.S. In fact, the U.S. previously established a baseline of legal rules for top-down privacy regulation in the Children's Online Privacy Protection Act of 1998 (COPPA), which attacked the "market's previous default of

---

[49] See Bronski, supra 10

[50] See Bronski, supra 10

[51] See Schwartz, supra note 815

maximum collection and use of children's personal information on the Internet"[52] by "prohibiting the take-it-or-leave-it notice and consent and in its place spelling out the elements required in order for notice to be valid for an informed consent."[53]

Similarly to COPPA, I believe the FTC is justified in establishing legal regulation of certain federally legislated required provisions that would prohibit mutable terms in the privacy policies that govern transactions online. In contrast to the private sector self-regulatory approach, the FTC can require Web sites to carry out the law since it has the legal power to enforce the required provisions.[54]

However, unless the required provisions are incorporated in federal legislation and enforced by the FTC under Section 5 of the Federal Trade Commission Act for deceptive online information practices, I think they would be the equivalent to the current voluntary recommendations and would provide no realistic privacy protection.

Moreover, it is necessary for the FTC to have the power to enforce privacy rights violations with sufficient remedies such as fines and potentially harmful bad publicity because Web sites that improperly collect personal information must fear that they will be publicly exposed and held accountable in a significant manner. Otherwise, the regulation would again prove to be ineffective and consumers will be forced to log off from the Internet or accept the current take-it-or-leave-it mutable terms that loosely secure their personal information.

---

[52] See Schwartz, supra note 815

[53] See Schwartz, supra note 815

[54] See Schwartz, supra note 815