3/26/2001

March 26, 2001

FTC VS. TOYSMART

While Toysmart generated a great deal of publicity and ignited strong feelings about Internet privacy, the case ended anti-climactically. FTC pressure ultimately forced Toysmart not to sell its database of customer information, but little legal groundwork was laid to prevent future distressed e-tailers (or their creditors) from trying to sell their customer lists.

I. Introduction

¶ 1 Last summer, Toysmart agreed to a settlement with the Federal Trade Commission concerning use of its customer information database. Under the terms of the settlement, the defunct Internet toy retailer was permitted to sell customer information without either providing its former customers notice or giving them an opportunity to block the sale or use of their personal information. This issue ignited a privacy-rights maelstrom, but ended anti-climatically for Toysmart; in January, Buena Vista Internet Group, a Disney subsidiary and 60% majority shareholder of Toysmart, agreed to compensate the company's creditors $50,000 for the privilege of destroying the database. U.S. Bankruptcy Court Judge Carol Kenner approved this plan, subject to the limitation that Toysmart attorneys must retain the list and destroy it (rather than physically transfer it to Buena Vista) when all creditor claims are satisfied.

¶ 2 Although amounting to less than 1% of the $18 million of creditor claims against Toysmart, the dollar value of the settlement belies the potential damage that the sale could have had on consumer confidence in online transactions. A successful sale of Toysmart's database could have paved the way for a horde of distressed e-businesses to sell what many consumers' consider their most valuable asset.

¶ 3 This brief will discuss the many implications of both the Toysmart/FTC settlement and the subsequent sale of Toysmart's customer information database. This issue has enormous potential to impact many parties: not just Internet consumers, but also any company with a web presence and information about its customers. U.S. government entities also have an important

stake in what these companies do with information obtained via the web, as they are the ultimate gatekeepers who must protect the interests of consumers while not stifling the burgeoning business of doing business on the net. While the potential impact on these diverse parties is interesting and important, we wish to focus on the impact of the Toysmart settlement on private sector online privacy watchdogs. These organizations play a special role in the Internet economy as champions of consumers concerned with the sanctity of information they provide over the web. The most prominent of these organizations, TRUSTe, certified that the information on Toysmart's site would never be sold. However, TRUSTe could not protect its certification by taking direct action to prevent Toysmart from selling its customer database and was ultimately forced to rely on the FTC's assistance.

II. Facts of the Toysmart/FTC Settlement

Toysmart: Defunct E-tailer

¶ 4 Until it ceased operations in May, Toysmart was a "virtual toy store"--an Internet retailer that sold toys via a website. The company was based in Waltham, MA, where it had a physical presence, but transacted business primarily on the website http://www.toysmart.com. Toysmart began advertising, promoting and selling toys online in January 1999. Months later, in September, Toysmart became a licensee of TRUSTe, an organization that certifies the privacy policies of online businesses and in turn allows such businesses to display a TRUSTe seal. In addition to obtaining a TRUSTe license and exhibiting its seal, Toysmart displayed the following language on its site indicating its 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."

¶ 5 After ceasing operations, Toysmart hired a consulting firm to assist with the sale of its business and/or remaining assets. It sought bids for various assets: customer lists, inventory, warehouse fixtures and equipment, intangible assets and business plan. The company's creditors petitioned for involuntary bankruptcy in early June; bids for Toysmart's remaining assets were required to be submitted ten days later.

What Privacy Information did Toysmart Possess?

¶ 6 While operating, Toysmart routinely collected personal information from customers, including names, addresses, billing information, shopping preferences and family profile information[1] Additionally, just a couple of weeks before ceasing operations, Toysmart began collecting personal information from children on its site through a dinosaur trivia contest. This information included names, ages and e-mail addresses of children. However, the contest did not include a mechanism for parental notification or consent prior to collection of this information.

What Violations Did the FTC Allege?

¶ 7 The FTC sued Toysmart to block the sale of its customer database, saying it violated consumer protection laws and the privacy rights of Toysmart's customers. The primary violation alleged by the FTC was against the prohibition of "unfair or deceptive acts or practices in or affecting commerce."[2]

What Remedy Did the Parties Ultimately Agree To?

¶ 8 The FTC wished to permanently enjoin Toysmart from selling its customer lists. Ultimately, the parties agreed to a quick settlement that has been criticized by many concerned with privacy policies of Internet companies. Under the terms of the settlement, Toysmart was allowed to sell its database but only to a "qualified buyer". The settlement agreement defined "qualified buyer" as an entity engaged in the family commerce market that expressly agrees to be Toysmart's successor-in-interest to the information contained in the database. This means that the purchaser must be in the same line of business as Toysmart--presumably the business of selling toys on the web. Significantly, the agreement did not require the ultimate purchaser to provide Toysmart customers with either notice or the ability to "opt out" of transferring personal information to it.

¶ 9 As it turns out, the validity of this agreement was not significantly tested in court. Had Toysmart sold the database to an independent entity and "qualified buyer", a bankruptcy judge would have had an opportunity to set other conditions on the sale. When Toysmart agreed to sell to Buena Vista (who would then destroy it), Judge Carol Kenner allowed this sale to Toysmart's largest shareholder, but set a condition that Toysmart couldn't physically transfer the database; Toysmart must destroy the database itself. We will never know what conditions the court might have imposed had Toysmart sold to an independent entity.

III. Implications for the Privacy Rights of Internet Users

How Deep are User Concerns about Privacy?

¶ 10 Internet users are undoubtedly concerned about how companies use the data that they provide via the web, and this deep mistrust of online vendors is evidenced by a wide variety of studies. One study found that the sale of personal information was the most pressing privacy concern for Internet users--42% of all respondents cited this concern,[3] 87% of those queried in a different survey objected to websites selling their personal information to other businesses.[4] Even when companies merge, 71% of persons polled believe merging companies should obtain express written permission prior to sharing customer data. Indeed, a strong majority (64%) of those surveyed do not even trust sites that post a privacy policy.[5] Thus, if distressed e-commerce companies like Toysmart are able to sell data that they previously assured was not to be shared, it could serve to exacerbate consumer mistrust of websites' privacy policies, already a pressing concern.

How Important are Privacy Concerns for the Ultimate Success of E-tailing?

¶ 11 As previously evidenced, privacy concerns are perhaps the most important reason why people do not use (and therefore do not shop on) the Internet. Undoubtedly, privacy worries have significantly hurt revenue streams and have already resulted in untold lost profits for e-tailers. According to the Center for Democracy and Technology, such concerns resulted in $2.8 billion in lost online retail sales in 1999 alone, and will total $18 billion in three years if no changes are made to further protect the privacy of consumers' personal information.[6] Consumers apparently have an expectation that certain types of data will remain private. While online sales will likely continue to grow despite the aforementioned concerns, the pace will largely be determined by the degree to which e-tailers can boost consumer confidence in the medium. As the next section discusses, litigation may also play a critical role in the privacy policies of e-tailers in the future.

IV. Legal Analysis of Violations of Privacy Policies

E-tailing, Privacy and Litigation

¶ 12 With increasing frequency, litigation is being utilized as the tool to protect the privacy rights of Internet users. Attorneys General are beginning to target and prosecute e-tailers that violate their privacy promises. Following the Toysmart settlement, forty-seven Attorneys General filed an objection to the terms in which they promulgated a privacy agenda demanding that customers be allowed to opt-in as indicia of their consent to a sale of their customer

database to a third party. While the resolution of the Toysmart case circumvented this issue, it will surely be raised again in the near future.

¶ 13 Of course, Toysmart is not the only Internet business subject to recent litigation alleging consumer privacy violations. For example, Doubleclick is currently involved in a class action suit that alleges the company misused or monitored confidential customer information in the course of delivering advertisements on the Internet.[7] Additionally, Amazon has been the subject of litigation concerning its alleged impermissible collection of personal information from customers.[8] How might plaintiffs allege a privacy violation? The next section discusses some possibilities.

How Might a Plaintiff Challenge an E-tailer's Privacy Policy?

¶ 14 First, a plaintiff may argue that a web site's privacy policy is part of the contract with the customer, and a violation of that policy thus constitutes a breach. To succeed on a breach of contract theory, however, the plaintiff must show that the privacy policy is a contract between the web site and the customer. The Uniform Commercial Code provides that the contract of the parties "means the total legal obligation which results from the parties' agreement as affected by the Act and any other applicable rules of law."[9] According to the UCC, the "agreement" means "the bargain of the parties in fact as found in their language or by implication from other circumstances including course of dealing or usage of trade or course of performance."[10] The plaintiff would need a compelling argument that a web site breached the contract if the agreement contains language incorporating by reference the policies of the company. In the absence of such language, the plaintiff would have to rely on usage of trade, course of dealings, or course of performance. "Usage of trade" means a practice "having such regularity of observance ... as to justify an expectation that it will be observed with respect to the transaction in question."[11] Whether a privacy policy comes within this definition will depend on the future status of privacy policies. "Course of dealings" refers to an understanding between parties based on past transactions between the parties.[12] "Course of performance" refers to the parties' performance of the contact at issue.[13] A privacy policy is likely to meet one of these standards.

¶ 15 Another option for a potential plaintiff is common law misrepresentation. To succeed on this claim a plaintiff must prove justifiable reliance upon the misrepresentation of the web site's privacy policy.[14] The requirement of justifiability refers to whether the representation relates to a matter about which a reasonable person would attach importance in deciding upon a course of action.[15] In other words, the fact represented must be a material one. The

determination whether the statement might justifiably induce the action is a matter the jury must frequently consider.[16] Courts have held that materiality will be found where the representation was one of the grounds but not necessarily the sole ground that caused the plaintiff to act.[17]

¶ 16 A plaintiff may also allege a violation of a particular state's Deceptive Trade Practice Act. In general, to prove this claim, the plaintiff would have to show that the web site had knowledge of the deceptive trade practice or that the site had a financial interest in the goods or services deceptively offered for sale.[18] A plaintiff could prove that the site knew of the deceptive trade practice by showing that it entered into a business arrangement whereby, despite a privacy policy, the web site shared customer information with another company. Furthermore, the plaintiff could demonstrate that the web site had a financial interest in the information shared by proving that it profited by the sale.

¶ 17 As a fourth alternative, a plaintiff may allege a violation of the common law right to privacy, specifically the intrusion upon seclusion.[19] The standard for intrusion upon seclusion is "intentional intrusion, physically or otherwise, upon the solicitude or seclusion of another in his private affairs...if the intrusion would be highly offensive to a reasonable person."[20] A plaintiff could claim that the intrusion upon private affairs was the sale of customer information. A problem with this claim is that typically the information is willingly furnished, not secretly procured. A plaintiff may be able to counter this by arguing that the site's confidentiality policy was misleading.

V. Implications for Privacy Watchdogs (TRUSTe)

¶ 18 Among online privacy watchdogs, TRUSTe is perhaps the most recognizable and significant group attempting to ensure that government does not exert its legislative muscle in order to regulate online privacy. TRUSTe's licensees include all of the Internet's portals, three-quarters of the top twenty sites and roughly half of the top one hundred sites.[21] Indeed, in a study conducted by Cheskin Research, the TRUSTe's mark was ranked as the most trusted symbol on the Web among U.S. Internet users.[22] Given its dominant presence among those concerned with online privacy, TRUSTe's actions and policies have been the focus of a great deal of attention, some of which has been critical. Already facing criticism for its history of being "toothless" in its enforcement against its licensees, TRUSTe's inability to foil Toysmart legally without the assistance of the FTC may indicate a future shift in reliance to alternate ways of monitoring and enforcing the privacy policies of e-tailers.

History of TRUSTe: Independent Watchdog or Sponsor Puppet?

¶ 19 Founded in 1997 by the Electronic Frontier Foundation (EFF) and CommerceNet as a non-profit organization, TRUSTe derives almost half of its income from licensing.[23] However, TRUSTe's initial backing during its infancy was financial support from such corporate giants as Microsoft, RealNetworks, and America Online. Ironically, TRUSTe also counts each of its principal corporate backers among its clients - all of its sponsors are also certified and licensed to use the TRUSTe logo on their websites.

¶ 20 In March 1999, TRUSTe was forced to grapple with the issue of independence when Microsoft was discovered to be compromising consumer trust and confidence through its use of "global unique identifiers" in its Windows 98 registration process. Consumers who declined to release information during the online registration process were still in fact submitting information to Microsoft. Faced with the dilemma of whether to revoke the certification of one its primary sponsors, TRUSTe declined to do so on the grounds that there was no privacy violation since TRUSTe's certification was seen as only extending to its website Microsoft.com and not specific Microsoft applications. In a similar situation last year involving RealNetwork's RealJukebox, TRUSTe used a related argument to decline to revoke its corporate partner's license to use the TRUSTe logo. As a result, TRUSTe has often been criticized for being unwilling to reprimand and revoke its licenses for fear of losing its funding. This criticism weakens its ability to credibly bill itself as an independent watchdog over the Internet and its licensees.

¶ 21 In the face of such criticism, TRUSTe has fought to maintain and improve its reputation. In light of the Microsoft incident, TRUSTe recently announced that it would expand its policies to cover both software and third party involvement in licensed sites. In addition, it has taken legal action against a former licensee that continues to use its TRUSTe logo after its agreement with the organization lapsed.[24] Just recently, TRUSTe brought suit against a political website that was using a facsimile of its trust mark without permission.[25] Such defensive measures to protect its reputation and intellectual property should help TRUSTe gain legitimacy as a protector of privacy rights.

Legal Recourse of Online Privacy Seals

¶ 22 Recent changes implemented by TRUSTe fail to address the fundamental problem with online privacy seals: the lack of effective recourse by the organization itself against violators of its certifications. TRUSTe's website suggests that it has two legal methods of enforcement for sites that violate its licensing agreement: revocation of the use of its trademark

and breach of contract. Although these two sources of action may occasionally be sufficient, the organization remains primarily dependent upon third parties such as the FTC, Attorneys General, and the CPA. This is evidenced by TRUSTe's reliance on the FTC in the Toysmart case.

TRUSTe: Watchdog, Liaison or Enforcement Agency?

¶ 23 Many acknowledge TRUSTe's lack of power by insisting that its role is not as an enforcement organization but is instead as a "liaison" or "watchdog".[26] As such, its role in online privacy is uncertain. Indeed, some have dismissed TRUSTe's actions in the Toysmart case as nothing more than a public relations gesture.[27]

¶ 24 If TRUSTe's vision of self-regulation is to succeed, the FTC may have to pressure online privacy groups to take a more aggressive stance. As Mark Plotkin, an attorney expert in this area, notes, "one of the solutions short of legislation and regulation is to look to the FTC to hold privacy seal [organizations] like TRUSTe ...to enforce privacy seal commitments."[28]

¶ 25 Such enforcement would require providing a more effective legal recourse against violators. To date, federal sources of authority have been limited and there has been little consistency in the federal approach to regulation. Given that e-commerce applications often transcend jurisdictional boundaries, there may be varying standards of governing privacy law. TRUSTe's ability to enforce its agreements with licensees may turn on privacy law nuances. Ironically, in its effort to head off government regulation of online privacy, TRUSTe may have been preventing itself from gaining the sort of regulatory muscle that it needs to enforce its agreements.

The Future of TRUSTe

¶ 26 Although TRUSTe's actions to date have mainly been limited to revocation of licensee's rights, breach of contract and referral, this may soon change. As the federal government begins to scrutinize online privacy rights, TRUSTe's role in the realm of online privacy regulation may turn from liaison or watchdog to enforcer. With its prominent position in the marketplace and high level of recognition by a large number of web users, TRUSTe has an excellent opportunity to gain the enviable position of the ultimate enforcer of Internet users' rights. Indeed, its seal is valuable intellectual property that it is willing to go to court to protect. TRUSTe's next step should be aggressive legal action to protect its legitimacy as a champion of privacy rights on the Internet.

VI. Conclusion

¶ 27 Toysmart is just the first case in what may soon turn out to be a wealth of litigation and regulation that will define the responsibilities of commercial entities on the web with respect to privacy. The case generated a great deal of publicity and ignited strong feelings on both sides of the many issues it raised, yet ultimately ended somewhat anti-climactically. As it turns out, Toysmart will not sell its database of customer information, but little legal groundwork has been laid to prevent other distressed e-tailers (or their creditors) from trying to do the same thing. Perhaps the strongest impediment to such an action is the potential for negative publicity, such as Toysmart and its affiliate Disney received over the past year. Perhaps the most interesting development of the case will be its effect on the nature of enforcement of privacy promises on the web. Will organizations like TRUSTe toughen up and demonstrate an ability to handle the task without government intervention? Or will the federal government and the courts need to play a larger role in enforcement of what is the biggest wild card influencing the long-term success of electronic commerce - consumer concerns about privacy?

By:
Daniel Bronski
Conway Chen
Matthew Rosenthal
Robert Pluscec

Footnotes

1. http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm
(visited March 26, 2001)

2. 15 U.S.C. §45(a)

3. Center for Democracy and Technology, *Survey Information: Americans Care Deeply About Their Privacy*, http://www.cdt.org/privacy/guide/introduction/surveyinfo.html
(visited March 26, 2001)

4. *AARP Members' Concerns About Information Privacy*, http://research.aarp.org/consume/dd39_privacy.html

(visited March 26, 2001)

5. Center for Democracy and Technology, *Survey Information: Americans Care Deeply About Their Privacy*, http://www.cdt.org/privacy/guide/introduction/surveyinfo.html (visited March 26, 2001)

6. Id.

7. *In Re Doubleclick Privacy Litig.*, 2000 U.S. Dist. LEXIS 11148 (J.P.M.L. 2000)

8. *In Re Amazon.com, Inc*, 2000 U.S. Dist. LEXIS 8201 (J.P.M.L. 2000).

9. U.C.C. §1-201 (11)

10. U.C.C. §1-201 (3)

11. U.C.C. §1-205(2)

12. U.C.C. §1-205(1)

13. U.C.C. §2-208(1)

14. Restatement (2nd) of Torts, §537

15. Restatement (Third) of Torts §538(2)(b)

16. Prosser and Keaton, *Prosser and Keaton on Torts* 5th Ed. P. 754

17. *Bond Leather Co., Inc. v. Q.T. Shoe Mfg. Co.*, Inc., 764 F.2d 928 (1st Cir., 1985)

18. *Aequitron Med., Inc. v. CBS, Inc.*, 964 F. Supp. 704 (S.D. N.Y. 1997)

19. Restatement (2nd) of Torts §652B

20. Id.

21. *TRUSTe Ranked Most Trusted Symbol on the Web*, PR Newswire, Aug. 14, 2000, *available in* LEXIS, Wire Service Stories, News

22. http://www.cheskin.com/think/studies/trust2.html
(visited March 26, 2001)

23. http://www.computeruser.com/magazine/national
/1803/covr141803.html
(visited March 26, 2001)

24. Alex Lash, *Enforcement: TRUSTe Muscles Up,* The Industry Standard, Apr. 3, 2000

25.
http://news.cnet.com/news/010052003295970.html
?tag=st.ne.1005.saslnk.saseml
(visited March 26, 2001)

26. *See* Linda Lee Larson & Steven D. Hall, *Website Certification: the TRUSTe Alternative,* CPA Journal, June 1, 2000

27. *See* Tom Kirchofer, *Value of Web Privacy Seals Questioned,* Boston Herald, July 31, 2000

28. Drew Clark, *Privacy: FTC Urged to Pressure Privacy Seal Groups*, National Journal's Technology Daily, July 18, 2000