# GOOD COMPUTING: A VIRTUE APPROACH TO COMPUTER ETHICS

A book under contract with
Jones & Bartlett Publishers
40 Tall Pine Drive
Sudbury, MA 01776
http://www.jbpub.com/

**DRAFT FOR**
**June Puerto Rico writing retreat**

**A section of Chapter 7**
***Privacy: Toysmart***
**Version 1: 4/17/07 by Chuck Huff**

Based on writings in www.computingcases.org prepared by Chuck Huff and Bill Frey and class documents from University of Mayaguez, PR, FILO 3185 prepared by Bill Frey

## Toysmart.com Abstract

Toysmart.com was a Disney-owned company that had been advertising, promoting, and selling toys on-line since January 1999. On May 22, 2000 Toysmart.com announced that it was going out of business and sought the help of a consulting firm, The Recovery Group, to confer in selling its assets. It was also on this date that advertisements began appearing in the Wall Street Journal and the Boston Globe in which Toysmart.com offered to sell its customer's personal information including consumers' names, addresses, billing information, and family information.

This case provides an invaluable tool for looking at privacy issues in computing not only because it sets a precedent for other failing on-line that they must maintain the rights of their consumers even if they are forced to file for bankruptcy. The Toysmart case also brings into question issues of honesty and deception in that toysmart.com was a licensee of TRUSTe, an organization that ensures that the privacy policies of on-line companies are maintained, and displayed its seal and trademark stating "Your information is safe with us!" on its website while advertising to sell its consumers' private information only months later as the company was forced into bankruptcy.

**Toysmart.com: Issues of Privacy and Deception**

People have traditionally held privacy as a precious commodity. Whether it is a social security number, credit card number, age, or favorite kind of toy, the information that helps give a person a feeling of personal identity is priceless. The activities surrounding the bankruptcy of online business Toysmart.com has had a dramatic effect on how information that has traditionally been considered private is able to be viewed—namely, as a marketable and lucrative business asset.

There is a high demand for electronic retailers (also referred to as "e-tailers") to create a shopping environment that meets the individual needs of each person who visits their website. In this way, a customer is shopping at his/her own personalized location. But how can online businesses persuade their customers to disclose their personal information? Although some studies have shown that the majority of individuals who use the Internet are concerned about the safety of giving away their personal information (AT&T Labs, 1999), Professor Mary J. Culnan, Director of the Georgetown University Internet Privacy Policy Study, has provided evidence indicating that websites have apparently have little to no problem obtaining personal information from individuals visiting their website. According to Culnan, "98% of the Top 100 websites collected at least one type of personal identifying information (e.g. name, e-mail address, postal address), 75% collected at least one type of demographic information (e.g., gender, preferences, Zip code) and 74% of the sites collected both personal identifying and demographic information" (Burka, 2001).

Toysmart.com did not stray from the norm in collecting personal information from their customers. Although Toysmart collected extensive personal information from their customers, great efforts were made to ensure customers that their information would remain securely confidential. There was an entire portion of their webpage devoted to showing website visitors the importance Toysmart placed on their customers' privacy. It was on this portion of the website that Toysmart displayed the prestigious TRUSTe stamp of approval it had earned as a result of its efforts to ensure privacy to their customers. Toysmart also pledged that they would "never share [their customers'] information with a third party." It was this was the privacy policy that may have helped solicit customers to shop at the website and join "Mytoysmart" as members.

Faced with immense debt as a result of an overestimate of profits to be gained from Christmas sales, Toysmart was faced with an ethically difficult choice. As an online company, Toysmart did not have the same type of material assets that are most commonly associated with bankrupt businesses. There were few tangible assests such as warehouses full of toys to be sold to the highest bidder. Instead, Toysmart was a faced with the reality that the bulk of their assets lay in the information they had obtained from their customers. Based on these factors, Toysmart was faced with a complex situation. They could either choose to abide by their promise to never share their customers' personal information with a third party and maintain their millions of dollars worth of debt, or they could advertise to sell the customer information and have the possibility of lessening their debt.

Reference:

M. J. Culnan, Georgetown McDonough School of Business, Georgetown Internet Privacy Policy Study,
available at http://www.msb.edu/faculty/culnanm/gippshome.html (current 6 Aug. 2001).

**Toysmart.com and TRUSTe**

Toysmart.com advertised, promoted and sold its products on-line while being licensed of the TRUSTe Privacy Program, whose primary purpose is to ensure that consumers' privacy rights are respected and that organizations follow their privacy policies. This allowed toysmart.com to display the TRUSTe trademark on their website, indicating to customers that toysmart.com was a company with which their personal information would be safe.

However, toysmart.com decided that displaying the TRUSTe trademark on its site did not fully explain the extent to which consumers who shopped at toysmart.com could be assured that any information that they disclosed while purchasing products from toysmart.com would remain secure and would at no time be shared with a third party. To this end, toysmart.com devoted a separate portion of their website to convey their promise to protect their consumers' private information including:

- Name
- Address
- Billing information
- Shopping preferences
- Order history
- Gift registry
- Selections
- Family profile information
- Specific information about consumers' children (e.g., name, gender, birthday, and toy preferences

How does a company become a TRUSTe licensee?

The United States District Court of Massachusetts found that toysmart.com had violated the Children's Online Privacy Protection Act ("COPPA") because it collected personal information from children under the age of 13 without requiring parental consent. This was in direct relation to the contests toysmart.com held on its website that children could enter by electronically sending their name and age. Parents were sent electronic mail informing parents that their children had entered a contest and parents of children who had won a particular contest were asked to report the child's address so that the child could receive his/her prize.

In lieu of toysmart.com's solicitation of offers for the purchase of toysmart.com's assets, including, but not limited to, Customer Lists and the personal information contained and ostensibly protected therein as was stated in their privacy statement, the United States District Court of Massachusettes found that toysmart.com's actions "will injure customers throughout the United States by invading their privacy" (????).

**Toysmart.com, the Federal Trade Commission, and the State of Texas**

In such a complex case as Toysmart.com, it is essential to take into account all of the stakeholders upon whom the case has had an affect. Among the stakeholders are the plaintiffs, the Federal Trade Commission (FTC), and the defendents, Toysmart.com, Inc. and Toysmart.com, LLC, respectively. There are other important stakeholders that play a vital role in this case—namely, the customers. John Cornyn, Attorney General of Texas, brought to the forefront this issue to the forefront in asking the United States District Court of Massachusetts (the court in which the civil case took place) permission to intervene as a party-plaintiff.

Cornyn spoke on behalf of all Texas consumers stating that Toysmart.com should be obligated to afford its customers the opportunity to permit the sale or transfer of their personal information to another party, since the customers agreed to become involved with Toysmart.com in lieu of their Privacy Statement, which indicated they their personal information would "never be shared with a third party." This places Toysmart.com in a role in which they are not only acting in an unethical manner by selling its customers' personal information without their consent, but also presents the image of a company run without regard for willingly deceiving its customers.

**Toysmart and the Issue of Privacy**

People have traditionally held privacy as a precious commodity. Whether it is a social security number, restaurant preferences, age, or favorite kind of toy, the information that helps give a person a feeling of personal identity is priceless. The advent and widespread use of the Internet has changed how information that was once deemed private is able to be viewed—namely, as a marketable and lucrative business asset.

It would be inaccurate to label websites who obtain and sell personal information from their customers as acting with malcontent. There is a high demand for electronic retailers (also referred to as "e-tailers") to obtain information from individuals because retailers will be better able to meet the individual needs of each person who visits their website. It would intuitively follow that consumers will shop at websites that fulfill their individual needs more than websites that seem cold and impersonal. This would cause online businesses who are best able to meet their customers' individual needs increase their probability for generating a profit.

But how can online businesses persuade their customers to disclose their personal information? Although some studies have shown that the majority of individuals who use the Internet are concerned about the safety of giving away their personal information (AT&T Labs, 1999) Professor Mary J. Culnan, Director of the Georgetown University Internet Privacy Policy Study, has provided evidence indicating that websites have apparently have little to no problem obtaining personal information from individuals visiting their website. According to Culnan, "98% of the Top 100 websites collected at least one type of personal identifying information (e.g. name, e-mail address, postal address), 75% collected at least one type of demographic information (e.g., gender, preferences, Zip code) and 74% of the sites collected both personal identifying and demographic information" (Burka, 2001).

Although Toysmart collected extensive personal information from their customers, great efforts were made to ensure that customers' information would remain securely confidential. There was even an entire portion of their webpage devoted to showing website visitors the importance Toysmart placed on their customers' privacy. It was on this portion of the website that Toysmart displayed the prestigious TRUSTe stamp of approval it had earned as a result of its efforts to ensure privacy to their customers. Toysmart also pledged that they would "never share [their customers'] information with a third party."

Faced with immense debt as a result of an overestimate of profits to be gained from Christmas sales, Toysmart was faced with an ethically difficult choice. As an online company, Toysmart did not have the same type of material assets that are most commonly associated with bankrupt businesses. There were no warehouses full of toys or dozens of stores to be sold to the highest bidder. Instead, Toysmart was a faced with the reality that the bulk of their assets lay in the information they had obtained from their customers. Based on these factors, Toysmart was faced with a complex situation. They could either choose to abide by their promise to never share their customers' personal

information with a third party and maintain their millions of dollars worth of debt or they could advertise to sell the customer information and have the possibility of lessening their debt.

Reference:

M. J. Culnan, Georgetown McDonough School of Business, Georgetown Internet Privacy Policy Study,
available at http://www.msb.edu/faculty/culnanm/gippshome.html (current 6 Aug. 2001).

# Supporting materials

# TRUSTe Guidelines
# on
# Personally Identifiable Information Uses in Mergers, Acquisitions, Bankruptcies, Closures, and Dissolutions of Web Sites

Submitted for Public Comment on April 11, 2001

## TABLE OF CONTENTS

## Executive Summary

Four years ago, TRUSTe set out to build a framework of trust and confidence between companies and their customers. At the heart of its mission is the belief that in an increasingly connected world, consumers must have mechanisms that give them full control over their personal, private information so that they can protect their privacy. At no point is this protection more important than when companies undergo the difficult business transition of mergers, acquisitions and bankruptcies.

Following several high profile bankruptcy and privacy incidents and numerous requests by industry for guidance on the changed privacy climate, TRUSTe created the following guidelines to serve as an important navigation point for its licensees. These guidelines are rooted in the TRUSTe license agreement and, if followed, will ensure that companies maintain appropriate uses of consumer personal information.

Specifically, these guidelines point to the following:

- Mandated Third Party Oversight – The critical point in these guidelines is that personal information transfer requires third party oversight as an important check against the singularly focused demands imposed by creditors. In an era marked by increasing consumer vigilance over privacy, third party oversight in data transfer is mandatory to the trust equation.

- Consumer Notice and Choice – TRUSTe recommends that giving customers opt-in is the best method to retain full value of a customer database and extend trust to new users. Indeed, if a company has made the promise to never share personal information, then a change in data handling and uses *requires* consumer opt-in. In other situations, providing both an opt-out option and public notice will be sufficient.

- Privacy Policies Must Be Honored – The same promises a company makes while in business, must be honored when going out of business. Given the current sensitivities towards privacy protection, consumer are beginning to understand that third parties exist – in the form of seal programs and government bodies – to ensure the integrity of privacy promises. To that end, both parties, the buyer and the seller, have an obligation to the consumer.

Our goal with these guidelines is to strike a reasonable balance between consumer privacy rights and expectations and the business need to realize the full value of asset portfolios. In an economy valued by information, customer data is like gold and, as such, deserves enhanced protection.

**We want to hear from you**. TRUSTe will post these guidelines on our Web site for 60 days to gain public comment. We invite you to make recommendations by

emailing us at **MABComments@truste.org**. Following the public commentary period, we will issue a final version and distribute to our licensees.

Overview:
TRUSTe has created guidelines on appropriate uses of consumer personal information for its licensees that are

- merging,
- being acquired,
- selling all or substantially all the assets of a business unit
- involved in bankruptcy proceedings,
- dissolving or closing the company,
- purchasing a company with assets that include personally identifiable information (PII), or
- purchasing a database including PII

At the conclusion of these guidelines are several scenarios to provide companies with additional guidance on when notice and choice (opt-in versus opt-out) must be given to the customer. Because many scenarios are likely to exist, these guidelines should be read as general guiding principles rather than an all encompassing rule. As a rule of thumb, companies should contact their TRUSTe account manager for further guidance specific to particular situations.

**Fundamental Obligations**

1. Inform TRUSTe of impending business changes as they impact customers' personally identifiable information and privacy practices.

2. Provide your customers and/or users with notice of the upcoming change.

3. If you have promised never to share personally identifiable information with a third party, at a minimum you must provide an opt-in before the information is shared with that third party.

4. If you have indicated in your privacy statement that you may share information with third parties, you should provide notice and an opt-out before sharing the personally identifiable information.

5. If the company will be sold in total to a company in a similar line of business with the same privacy policy, give notice to the customer.

**Definition of Personally Identifiable Information**

As delineated in the TRUSTe license agreement, PII is defined as any information

(i) that identifies or can be used to identify, contact, or locate the person to whom such information pertains, or

(ii) from which identification or contact information of an individual person can be derived.

PII includes, but is not limited to: name, address, phone number, fax number, email address, financial profiles, medical profile, social security number, and credit card information. Additionally, to the extent unique information (which by itself is not PII) such as, but not necessarily limited to, a personal profile, unique identifier, biometric information, and/or IP address is associated with PII, then such unique information also will be considered PII.

PII does not include information that is collected anonymously (i.e., without identification of the individual user) or demographic information not connected to an identified individual.

# Selling PII as Part of a Merger, Acquisition, or Bankruptcy

Discussing these guidelines with your TRUSTe account manager and implementing the agreed upon steps is essential to ensure that full control over personal information is given to consumers so that they can protect their privacy. To remain in compliance with the TRUSTe program, it is essential that companies follow the guidelines below.

*Contacting TRUSTe:* In the event of a merger, acquisition, bankruptcy, dissolution, or closure, an organization must begin a review of its data handling practices by contacting its TRUSTe account manager. TRUSTe account managers are trained to guide companies through the steps needed to ensure consumer privacy protection. By following these guidelines, companies will also minimize any problems concerning PII collected through the Web site during the term of its license agreement with TRUSTe.

*Non-Disclosure and Confidentiality:* If the information regarding your business decision is not yet public and you make the appropriate notification to the account manager, then this information will not be shared outside of TRUSTe. Please note that TRUSTe's license agreement (section 11.B of License Agreement 6.0) provides that TRUSTe will keep confidential any information that is not public knowledge and is specifically requested to be kept confidential. Companies should specify to their account manager what information regarding the change in business operations and/or status should be kept confidential, including marking documents as "confidential."

**Mergers and Acquisitions**

In the event of a merger or acquisition, TRUSTe licensees should take the following steps:

1. Review privacy statement to determine promises made to Web site customers and users. The privacy statement will indicate the restrictions that will apply to the transfer of the personally identifiable information.

2. Inform your TRUSTe account manager of the company's upcoming changes before this information becomes public knowledge, if possible. Companies must contact TRUSTe at least 30 days prior to merging or acquiring the customer database. At that time, TRUSTe will require the appropriate documentation so that we are assured customers are given the 30 day notice required in the license agreement (License Agreement 6.0, Schedule A Section 3 B vii.).

3. Depending on the current privacy statement, companies must provide notice of the merger to all the customers and/or users and as necessary obtain consent for the transfer of personally identifiable information.

   Depending on the type of information collected via the Web site and the preferences requested by the individual, consent can be obtained through opt-out or opt-in mechanisms. With prior written approval from TRUSTe, some cases require only prominent notice for at least 30 consecutive business days prior to the completion of the assignment or transfer.

   Contact TRUSTe for guidance on the appropriate measures for your company's specific situation.

4. TRUSTe will need the following information to determine how to provide notice and appropriate choice:

a. official name of the new company,
b. effective date of the merger,
c. the planned uses by the new company of the personally identifiable information in the customer database,
d. the new company's intentions to adopt the privacy policies of the licensee, or whether the company will follow different privacy policies, and
e. whether the new company intends to maintain a relationship with TRUSTe. If the company does not intend to participate in the TRUSTe Privacy Seal Program, you should follow the termination procedures of section 5 of License Agreement 6.0).

5. Once the company determines the methods by which customers and/or users will be given notice and/or choice, send a copy of the intended notice and choice documentation to TRUSTe for final review and approval.

   **Remember: This is an administrative email and must not include marketing information.**

## *Bankruptcies*[1]

**NOTE**

TRUSTe must be contacted immediately if a licensee or one of its creditors files a bankruptcy petition. Failure to do so may result in additional scrutiny by TRUSTe and possibly include a Web community advisory, compliance escalation procedure, and objection with relevant bankruptcy court.

TRUSTe licensees must take the following steps:

1. Review the privacy statement to determine the promises made to Web site customers and users. The privacy statement will indicate the restrictions that will apply to the transfer of the personally identifiable information.

2. Inform TRUSTe of the company's upcoming changes before filing for bankruptcy.

3. Companies selling customer information as part of the asset portfolio must give all consumers a reasonable opportunity to prevent the sale of their personally identifiable information, if:

    a. The PII will be used or disclosed by the buyer for a purpose not outlined in the TRUSTe approved privacy statement,
    b. The PII will be used for a purpose unrelated to the primary purpose for which it was collected, or
    c. The company promised not to sell, rent, or share the personally identifiable information.

4. Once a buyer of the database is identified, you must contact TRUSTe to determine the necessary level of notice and choice.

5. TRUSTe will need the following information to determine the required levels of notice and obtaining choice.
    a. the name of the company purchasing the assets,
    b. the effective date of the merger,

[1] In developing guidelines for bankruptcies, we have closely followed the developments of the Toysmart.com case. Briefly, Toysmart.com, a TRUSTe licensee, intended to breach its privacy policy when it announced bankruptcy during the summer of 2000. Following the intended sale of its customer database, TRUSTe issued an advisory to the Web community stating that it would take all steps under the law to prevent any such exchange. In the wake of TRUSTe's legal actions, and those of more than 42 state attorneys general and the Federal Trade Commission, Toysmart.com ultimately destroyed the database with no transfer of information to a third party.

c. how the new company intends to use the personally identifiable information in the customer database,
d. whether the new company will be adopting the privacy policies of the licensee, or if it will have different privacy policies, and
e. whether the new company intends to maintain a relationship with TRUSTe, (if not, you should follow the termination procedures of section 5 of License Agreement 6.0).

6. Once you and your TRUSTe account manager determine how customers and/or users will be given notice and/or choice, provide TRUSTe with documentation of the notice and choice you intend to send to your customers prior to sending it.

**Remember: this is an administrative email and must not include any marketing information.**

**Dissolution or Closure of a Company**
In the event of a dissolution or closure, the TRUSTe licensee must take the following steps:

1. Determine whether PII will be sold as part of the closure or dissolution.
    a. If PII will not be sold, you need to inform your consumers of the impending change and whether the law requires maintaining or destroying the information.
    b. If PII will be sold as part of the dissolution or closure of the company, follow the steps outlined for a merger or acquisition [see page 8].

# Purchasing a List or Company through a Merger, Acquisition, Asset Sale, or Bankruptcy.

When it comes to consumer privacy, both the company being sold and the purchaser have responsibilities. If your company has decided to purchase a company or the customer database of a company that is a participant in the TRUSTe program, then it is important to remember what obligations are tied to the PII.

1. Review the privacy statement that governs the personally identifiable information to assess what promises were made to Web site customers. The privacy statement will indicate what restrictions will apply to the transfer of the personally identifiable information.

2. Determine whether the company from which you are purchasing the information has fulfilled its obligations to provide notice and/or choice to its customers and/or users.

3. If the company is a TRUSTe licensee, but your company is not, consider whether your company would like to join TRUSTe's Privacy Seal Program.
    a. If yes, your company will need to complete a new self-assessment document and undergo the certification process. Note: All TRUSTe licensees must give Web site customers and visitors notice, choice, access, security and redress in their privacy policy.
    b. If no, your company should ensure that the company from which the personal information is being purchased has gone through the appropriate steps with TRUSTe [see above sections]. Unless users are given appropriate notice and choice, you must follow the privacy policy under which it was collected and immediately provide customers with appropriate notice and choice.

4. Prior to the merging of your Web site customer or user databases with other databases, your company must send TRUSTe a letter dated and signed by an officer of the newly formed company. The letter should state:
    a. the merger is taking place,
    b. the name of your company,
    c. whether the sale is for a substantial portion of the assets or for just the customer and/or user list,
    d. the effective date of the merger,
    e. how the new company intends to use the personally identifiable information in the customer database,
    f. whether the new company will be adopting the privacy policies of the licensee, or if it will have different privacy policies,
    g. whether you intend to maintain a relationship with TRUSTe. If you do not intend to join the TRUSTe Privacy Seal Program, ensure the TRUSTe licensee has followed the termination procedures of section 5 of License Agreement 6.0),

h. If you choose to maintain your relationship with TRUSTe, there should be a location for TRUSTe's President and CEO to sign, agreeing to the assignment of the TRUSTe license agreement to the new company.

5. Companies intending to change the privacy practices must complete a new TRUSTe self-assessment form. You can download a new version of the self-assessment form from TRUSTe's Web site at www.truste.org.

6. If you have chosen to maintain a relationship with TRUSTe, then we will return a signed copy of the above letter, indicating our acceptance of the assignment.

**Scenarios Impacting Consumer Privacy: Notice and Choice**

While there are myriad permutations on how personal information can be transferred during a business transition period, we have highlighted a few recurring scenarios. These examples are meant to provide you with additional guidance on when notice and choice (opt-in versus opt-out) should be given to customers.

All of the examples pertain only to situations in which the majority of the assets that are being sold include personally identifiable information and are part of a merger, acquisition, bankruptcy, closure, or dissolution. Again, to ensure guidance on a particular situation not identified in these guidelines, companies should contact TRUSTe for clarity.

**NOTE**

A one time administrative email to your customer and/or user database to communicate the change in business may be sent. This administrative email may only be sent **once** and must not include **any** marketing material..

**Scenario 1: "We Will Never Sell Personal Information…"**

If your privacy policy states, "We will never sell, rent or lease your information" and you would like to sell the file or list of customer PII, then you need to provide at least 30 days of prominent notice on your Web site and send an administrative email with an opt-in for all consumers prior to selling the information.

**Scenario 2: "We May Share Personal Information With A Third Party…"**

If your privacy policy indicated that customer information may be shared with third parties, you need to provide at least 30 days of prominent notice on your Web site and send an administrative email with an opt-out for all consumers prior to selling the information.

**Scenario 3: "We Are Selling Most of our Assets to an Organization for Related Purposes…"**

If you are selling a substantial majority of the assets for a particular service, including the customer and/or user database, to an organization that will be using the database for related purposes and will maintain the same privacy policy, you must give 30 days prominent notice on the Web site prior to the transfer. In this instance you must receive written approval from TRUSTe.

Miscellaneous:

- If you are selling the list or database of customers and/or users as part of an asset sale, you must follow either example 1 or 2 above.
- If you are transferring information to a subsidiary, the rules outlined above apply.