The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?

Kalinda Basho†

The increase in the private sector's collection and use of individuals' personal information raises a new threat to privacy in the electronic marketplace. Each day, businesses are collecting sensitive information about consumers' buying habits, occupations, income, families and product preferences. This information is used to create customized advertising campaigns, make decisions about which customers to market products to and predict consumers' future purchases. Current solutions to online privacy fail to give consumers control over how their information is used or compensation for the data they share. This comment will propose that an online licensing system based on the Uniform Computer Information Transaction Act (UCITA) can achieve these objectives. Individuals will contract with businesses for the right to use their personal information. The licensing terms they negotiate will set limits on how their data is used, how long it is used and what type of benefit it is exchanged for.

---

† J.D. Candidate, May 2001, School of Law, University of California, Berkeley (Boalt Hall); B.A., University of California, San Diego, 1997. I would like to thank Professor Pam Samuelson for her insight, criticism and guidance. A very special thank you to Ashish Raina for his comments, suggestions and encouragement on this paper. I dedicate this paper to my parents, Surinder and Susan Basho, and sister, Surina Basho, for their support and love. Finally, I thank the members of the *California Law Review* for their helpful editing of this Comment.

They're watching you. Each time you view a Web page, enter an online contest, complete a Web site survey or purchase items they take note. Who are "they"? Often they are Internet Service Providers (ISPs),[1] marketers,[2] and businesses.[3] These entities want information that will let them know who you are, what type of products you buy, when you are most likely to buy them, and why.[4] By using your consumer profile, entities can determine how to effectively advertise to you and sell you more products. This type of exploitation of individuals' personal information,[5]

---

1. *See* Jesse Berst, *Day One of the Converged World* (visited Jan. 11, 2000) <http://chkpt.zdnet.com/chkpt.adem2fpf/www.anchordesk.com/story/story_4332.html>. The merger of AOL, an Internet Service Provider, with the media giant Time Warner will allow the two companies to combine AOL's online users' information with Time Warner's magazine subscribers' offline information to learn more about the behavior of their customers. Essentially the merger creates a "media company that watches and knows all." *Id.*

2. *See* Sandeep Junnarkar, *DoubleClick Accused of Unlawful Consumer Data Use* (visited Jan. 28, 2000) <http://news.enet.com/news/0-1005-200-1534533.html>. A California woman filed suit against DoubleClick, an online advertising firm, for unlawfully obtaining and selling consumers' private information. The company has formed alliances with online sites to create a network that allows it to track surfers' personal data and shopping habits. DoubleClick has stated that it plans to use this information to create a database of consumer profiles that will include "consumers' names; addresses; retail, catalog and online purchase histories; and demographic data." *Id. But cf. Statement From Kevin O'Connor, CEO of DoubleClick* (Mar. 2, 2000) <http://www.cdt.org/privacy/000302doubleclick.shtml>. DoubleClick's CEO announced that the company is committed to not linking "personally identifiable information to anonymous user activity across Web sites" until "there is agreement between government and industry on privacy standards." *Id.*

3. *See* Deborah Kong, *E-mergers Trigger Privacy Worries*, SAN JOSE MERCURY NEWS, Jan. 24, 2000, at 1E. The online company ValueAmerica has a database with details about the 600,000 members who used its site. *See id.* It used this information to increase sales by "identifying a shopper who . . . just bought a new DVD player and sending him an e-mail about the newest movies released on DVDs." *Id.* As the company now considers an acquisition, it recognizes that one of its most useful assets is its database of consumer information.

4. *See* Ken Magill, *Kmart, Yahoo Deal a Databaser's Dream?*, MARKETING NEWS, Dec. 24, 1999, at 1. Kmart and Yahoo! have teamed up to offer free Internet access and a co-branded shopping site. This partnership will allow the two companies to utilize real-world data Kmart has collected about 85 million households and apply it to target-based marketing on the Internet. Kmart chairman Floyd Hall stated that Kmart has the capability to figure out not only what type of toothpaste a consumer will buy but what brand, how much, and what items they will be interested in buying in the future. *See id. See also* Paulina Borsook, *The Uses and Abuses of Customer Profiling*, KNOWLEDGE MANAGEMENT, Nov. 1999, at 57 ("The business benefits of effective selling, targeting to individual consumer preferences and data mining for individualized selling are . . . overwhelmingly huge . . . .") (quoting Susan French, Vice President of Services, DataMain). For a more detailed discussion of consumer profiling on the Internet and an explanation of how it works, see Deirdre Mulligan, *Public Workshop on Online Profiling: Testimony of the Center for Democracy and Technology Before the Federal Trade Commission* (Nov. 30, 1999) (visited on July 15, 2000) <http://www.cdt.org/testimony/ftc/mulliganFTC.11.30.99.shtml>.

5. I use the term "personal information" throughout this paper to refer to any data voluntarily given or electronically collected about an individual on the Internet which can be directly linked to that person. This included, but is not limited to, an individual's name, address, telephone number, Social Security number, credit card numbers, Web site viewing habits (when linked to identifiable information provided by the user at registration), online purchases, and so forth. Personal information does not include pseudonymous or aggregate data that cannot be limited to a specific individual. This paper

without their consent or knowledge, leaves many Internet users feeling as if they have no privacy.

In the 1890 article *The Right to Privacy*, Samuel D. Warren and Louis D. Brandeis introduced the concept of a legal right to privacy.[6] They explained that the right to privacy constitutes the individual's right "to be let alone."[7] In the modern world of cellphones, email, videocameras, and Web site tracking mechanisms, the realization of this type of privacy is virtually impossible. As a result of intrusive technologies and sophisticated data collection systems, the right to privacy has shifted from an expectation of being "let alone," to a desire to control the flow of personal information. Privacy in the Information Age can best be defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[8]

Current American privacy laws and self-regulation principles fail to adequately protect information privacy for the following reasons: (1) they are not international in scope; (2) they do not provide a uniform system for protecting personal information privacy; and (3) they do not succeed in balancing consumers' interests in controlling uses of their information and benefiting from its disclosure with commercial entities' interest in obtaining and using that information. This Comment focuses on the final problem posed and argues that a licensing system could succeed in balancing the interests of consumers and businesses by allowing consumers to contract with commercial entities for the use of their personal information.[9] Consumers could specify in the license agreement the terms of use for their information and the form of compensation they expect to receive from the entity.

---

focuses on information about an individual that is transmitted over or created on the Internet. It therefore does not include information that only exists in the "real world."

6. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

7. *Id.* at 205.

8. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967). While Westin developed this defmition in 1967, before the Internet even existed, it has become a classic summation of information privacy and has been credited by Oscar Gandy as the most "well known definition of information privacy." Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace*, 1996 U. CHI. LEGAL F. 77, 117 (1996).

9. The concept for licensing personal information was first proposed by Lorin Brennan in his article *The Public Policy of Information Licensing*, 36 HOUS. L. REV. 61 (1999). He recognized that "standard-form licensing may become a valuable method for consumers to protect their privacy online" and suggested that this could be achieved under proposed Article 2B of the Uniform Commercial Code (U.C.C.). *Id.* at 62, 98-99. This Comment will expand upon Brennan's idea in two ways: (1) it will show how UCITA protects personal information in the way that Brennan suggested Article 2B could; and (2) it will show how UCITA could support a licensing system for online personal information.

The Uniform Commercial Information Transactions Act (UCITA) provides a framework for such a licensing system.[10] The National Conference of Commissioners of Uniform State Laws (NCCUSL) designed UCITA to create standard rules for transactions in software over the Internet, but its language is broad enough to encompass online products besides software, such as the personal information of Internet users. Under UCITA, individuals could create standard form licenses to govern the collection of their personal information as well as the benefit received for its disclosure,[11] such as customization of Web sites, services such as those provided by Hotmail[12] or Ecircles,[13] informational content,[14] and monetary compensation.[15] A licensing system might also force businesses to be more discreet in determining what information to collect and how to use it.

I have developed the following goals that I think an online privacy system should meet:

1. Choice: It must give individuals the choice of sharing or not sharing their information. If individuals decide to share their information, they should have the right to decide who receives what information about them.
2. Notification: It must inform consumers how their personal information is being used.
3. Verification: It must provide a means to verify that a business's privacy policies are followed.
4. Compensation: It must compensate individuals for the use of their personal information.
5. Ease of Use: It should not be so cumbersome that individuals are forced to choose between their privacy and their time.

---

10. UNIF. COMPUTER INFO. TRANSACTIONS ACT (Draft, July 1999). All drafts of UCITA are available from the Uniform Law Commissioner's official draft site (visited on July 16, 2000) <http://www.law.upenn.edu/bll/ulc/uk-frame.htm>.

11. This Comment is not meant to provide a solution for individuals who want to completely protect the privacy of their personal information. Rather, the objective here is to find ways for people to actually control the use and dissemination of their information while receiving some type of benefit in return.

12. Hotmail is a free email service on the Internet. To view this site, go to <http://www.hotmail.com>.

13. Ecircles is an Internet based application that facilitates group communication and allows users to share files. To visit this site, go to <http://www.ecircles.com>.

14. "Informational content" refers to information that is not purely marketing but is useful in some way. For example, many Web sites provide their viewers with health tips (<http://www.webmd.com>), cooking recipes (<http://www.ragu.com>), and even tooth brushing techniques (<http://www.crest.com>). Obviously, this type of benefit is difficult to define because it will vary from person to person.

15. Monetary compensation will most likely come from businesses that either do not have a web site at all and are only interested in collecting information on the Internet or have a site that offers the individual very little beyond product information. Sites that offer little beyond product information include typical online stores that are designed to sell items rather than inform or educate their viewers. See <http://www.macys.com> for an example.

6. Enforcement and Redress: It must have mechanisms in place to ensure compliance and recourse for injury.[16]

To evaluate the effectiveness of this system, it is important to first understand the problem it resolves. Part I describes the consumer and commercial interests at stake in the battle for control of individuals' personal information. The first Section will provide the context for this problem by evaluating the current market for personal information on the Internet. The second Section will discuss the values which individuals attach to privacy to explain why consumers should be allowed to control their data and profit from its use.

Part II will evaluate the effectiveness of the three privacy protection systems that are currently used in the United States: government regulation, self regulation, and technological solutions. This Part will demonstrate the failure of these privacy solutions to meet the six enumerated goals. Part III will argue that a licensing system designed to give individuals the ability to enter contracts with businesses for the use of their personal information will give individuals control of their personal information and the ability to profit from its use. This Part will consider the assumptions a licensing system is based upon and the potential problems with this solution. Part IV will show that UCITA provides a legal basis for a personal information licensing system. It will discuss the framework UCITA sets out for issues of liability, contract formation, and warranty in information licenses. This Part also will consider the problems with the application of UCITA to personal information licenses such as the Act's limited jurisdiction and ineffective remedies for breach of contract. Finally, Part V will consider whether an information licensing system will be able to achieve the goals of Internet privacy. Additionally, it will assess some of the consequences of this system in terms of socioeconomic stratification and information protection in the offline world.

I

COMPETING INTERESTS IN THE ELECTRONIC MARKET FOR PERSONAL INFORMATION

A. *Commercial Interests in Online Personal Information*

Commissioner Sheila Anthony of the Federal Trade Commission (FTC) was "shocked to discover" that an information broker in the offline

16. The FTC has designed a more detailed set of standards for privacy protection called the *Fair Information Practice Principles*. *See* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESSS 7-14 (1998) [hereinafter FTC REPORT]. While these do not serve as a complete standard for evaluating a system that compensates consumers, it does set a workable set of objectives for privacy protection on the Internet. The five elements of this policy are: (1) Notice and Awareness; (2) Choice and Consent; (3) Access and Participation; (4) Integrity and Security; and (5) Enforcement and Redress. *See id.*

marketplace had her and her husband's names, address, social security numbers, mothers' maiden names, children's and grandchildren's names and even the value of their home.[17] This type of "real world" information can be combined with our Web site viewing habits, chat line activity, and Web site registration data to create a profile of who we are.[18] In her testimony before the Subcommittee on Telecommunications, Trade and Consumer Protection, Deirdre Mulligan of the Center for Democracy and Technology identified this threat and suggested the need for a solution:

> The Internet accelerates the trend toward increased information collection that is already evident in our offline world. The trail of transactional data left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. When aggregated, these digital fingerprints reveal a great deal about an individual's life. The global flow of personal communications and information coupled with the Internet's distributed architecture presents challenges for the protection of privacy. . . . As we move swiftly toward a world of electronic democracy, electronic commerce and indeed electronic living, it is critical to construct a framework of privacy protection that fits with the unique opportunities and risks posed by the Internet.[19]

The Internet not only allows for faster collection of information, but also for the collection of more detailed information. Beyond data such as name, address, sex, date of birth, and Internet surfing habits, Web sites can collect detailed information about how we think or feel. This information about our thoughts or feelings is collected when we use "clever interactive tools such as Reel.com's Mood Matcher—which helps customers find movies based on their moods."[20] These services allow businesses to obtain highly intrusive psychographic data that would be difficult to collect and update through offline methods such as standard registration forms. Such information can then be combined with cookies,[21] third party data[22] or

---

17. *See Electronic Commerce: The Current Status of Privacy Protections for Online Consumers: Hearings Before the Subcomm. on Telecomm., Trade, and Consumer Protection of the House Comm. on Commerce*, 106th Cong. 40 (1999) (statement of Hon. Sheila F. Anthony, Comm'r, FTC).

18. *See generally* REGINALD WHITAKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY (1998) (looking at the threats that information technologies pose to privacy). Whitaker provides an insightful analysis of how personal information in both the offline and online worlds can be combined to create detailed profiles of individuals.

19. *Electronic Commerce: The Current Status of Privacy Protections for Online Consumers: Hearings Before the Subcomm. on Telecomm., Trade, and Consumer Protection of the House Comm. on Commerce*, 106th Cong. 83 (1999) (statement of Deirdre Mulligan, Staff Counsel, Center for Democracy and Technology).

20. Chet Dembeck, *Report Labels Internet Privacy Polices 'A Joke'* (visited Nov. 16, 1999) <http://www.ecommercetimes.com/news/articles/990916-3.shtml>. Reel.com has since taken this tool off its site, but users were able to type in their mood and receive a list of movies that "matched" it.

21. Cookies are small data files placed on an Internet user's hard drive when she first visits a site. The file includes information about where the user went on the Web site and the ads or content she

information a user provides when registering with the site. Using this data, organizations gain insight into a customer's motivations, desires, and interests.[23]

The Clinton Administration has recognized the intrusive nature of the Internet. The President has stated that Internet users should be able "to obtain relevant knowledge about why information is being collected, what the information will be used for, what steps will be taken to protect that information, the consequences of providing or withholding information, and any rights of redress that they may have."[24]

Unfortunately, this ideal is not a cyberspace reality. A 1998 FTC study of 1,400 Web sites revealed that only fourteen percent of these sites gave consumers notice of their information practices.[25] Additionally, the survey revealed that individuals often do not know whether their information will be transferred to a third party.[26] The market's failure to provide

---

saw. When that person returns to the same site, the site's computer server can read the usage data from the cookies and begin to compile more information about the individual's use of the site. Cookies are considered pseudo-anonymous trackers because they capture information about an individual's usage but they never reveal any identifying information such as a person's name, address or Social Security number. *See Cookie Central* (visited July 15, 2000) <http://www.cookiecentral.com>.

22. *See* Berst, *supra* note 1 (discussing how online information and data sold to sites by third parties is being used to create more personalized advertisements for Internet users).

23. This type of "consumer profiling" can be done by DoubleClick. The company is able to deliver real time marketing information about Internet users to its subscriber companies. The system works in the following way: when you log on to a site that has subscribed to DoubleClick's service, the site requests a cookie from your computer and gets any information in your cookie file. The site then sends a request to DoubleClick with your ID, requesting all available marketing information about you. This system makes it possible for a site to deliver specially targeted marketing banners to you while you are on their site. For more information on DoubleClick and its marketing techniques, see *Find Out How You Are Traced While Surfing on the Web* (visited Feb. 1, 2000) <http://www.cookiecentral.com/dsm.htm>; *see also* Barbara S. Wellbery, *Cyberspace and the Law*, 11 ST. JOHN'S J. LEGAL COMMENT. 659, 661-62 (1996) (stating that online and offline information "can be very revealing of one's personal habits when compiled and collected from many sources. For example, it is possible to infer a person's political or sexual leanings from the places they visit on the 'Web,' and to know when they are home and/or awake, and to discover who their friends and relatives are . . . "). Junnarkar, *supra* note 2.

24. President William J. Clinton & Vice President Albert Gore, Jr., *A Framework for Global Electronic Commerce* (visited Apr. 6, 2000) <http://www.iitf.nist.gov/eleccomm/ecomm.htm>.

25. *See* FTC REPORT, *supra* note 16, at ii-iii. Another report implies that the industry is getting better at providing effective information privacy policies. *See* MARY J. CULNAN, GEORGETOWN INTERNET PRIVACY POLICY SURVEY (1999). The survey found that of the 361 sites surveyed, 238 (65.9%) posted at least some type of a privacy disclosure. *See id.* at 8. Of the 236 Web sites surveyed that collected personal information and posted a privacy disclosure, 89.8% gave notice about at least one of the following issues: what information was being collected, how the information was being collected, how the information would be used, and whether the information would be reused or disclosed to third parties. *See id.* at 9. However, one should be skeptical of these findings. Not only was the survey sponsored by businesses with a stake in the outcome such as America Online or eBay, but it also tested a limited number of sites and failed to evaluate how informative or useful the explanations provided by the Web sites are. To see the survey in its entirety, go to the *Georgetown Internet Privacy Policy Study* (visited July 15, 2000) <http://www.msb.edu/faculty/culnanm/gippshome.html>.

26. *See* FTC REPORT, *supra* note 16, at 30. Currently, few Web sites actually disclose to consumers whether or not the information they provide could potentially be transferred to third parties.

consumers with adequate control over their personal information undermines consumer confidence in e-commerce.[27] Therefore, businesses can increase online commerce by creating and abiding by fair privacy policies. In fact, the Internet marketplace is beginning to realize that "[g]ood privacy practices are good business."[28]

In order to promote the growth of e-commerce, we need to find solutions that not only make consumers comfortable about sharing their information on the Internet but also fairly compensate them for the information they divulge. Internet users often are more willing to share their personal information if they receive a benefit in exchange for the privacy they surrender.[29] Many users have agreed to reveal information to advertisers such as who they are and where they go on the Internet in exchange for free

---

The FTC reported in its study that only 26% of the Health Sample sites (137 sites operated by "drug manufacturers, doctor's offices, hospitals, outpatient clinics, health maintenance organizations, manufacturers and retailers of health care products and non-prescription drugs, sellers of national supplements, weight loss centers, substance abuse treatment centers, and health information and referral services"), 33% of the Retail Sample sites (142 sites selling everything from photographic equipment to cigars and clothing), and 40% of the Financial Sample sites (125 sites operated by banks, credit unions, mortgage companies, venture capital firms, and other similar financial institutions) stated that at least some of the information they collected might be released to third parties. *Id.* at 21, 22, 30.

27. *See* Heather Green, *A Little Net Privacy, Please*, BUSINESSWEEK, March 16, 1998, at 98. A survey conducted by Louis Harris & Associates regarding Internet Privacy confirms that Americans care deeply about their privacy and that their concerns about the lack of privacy online are keeping many of them from ever venturing onto the Internet. The poll reveals that almost two-thirds of non-Internet users would be more likely to start using the Internet if the privacy of their "personal information and communications would be protected." Louis Harris & Associates, *E-Commerce & Privacy: What Net Users Want* (June 1998) (visited July 15, 2000) <http://idt.net/~pab/pabsurve.htm>. Privacy was the number one reason individuals stated for choosing to stay off the Internet, coming well ahead of cost, concerns with complicated technology, and concerns with unsolicited commercial email. *See* Green, *supra*. Of those surveyed who do use the Internet, 57% indicated that "web site policies that guarantee the security of their personal data affect their decision to make online purchases." *Id.* These results show that online privacy is a significant factor in an individual's decision to participate in the online environment and in e-commerce.

28. Borsook, *supra* note 4, at 63 (quoting Beth Givens, director of the Privacy Rights Clearinghouse, a nonprofit organization designed to inform individuals of their privacy rights). Christine Varney, advisor to the Online Privacy Alliance and a former FTC Commissioner, made the same point. "Businesses understand that these concerns are a top barrier to the continued growth of e-commerce and are putting their considerable advertising budgets behind increasing consumer privacy online." Steve Barth, *Is Self-Regulation Working?*, KNOWLEDGE MANAGEMENT, Nov. 1999, at 63 (quoting Christine Varney); *see also* Joel Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 772 (1999) ("Privacy is a critical issue for the growth of electronic commerce. . . . The fair treatment of personal information and citizen confidence in such treatment are necessary conditions for electronic commerce over the next decade.").

29. *See Web Privacy? Let's Make A Deal*, PALM BEACH POST, Aug. 26, 1999, at 4E; *see also Freebies for Personal Data OK*, USA TODAY, Sept. 14, 1999, at 1B (finding that when asked whether they would consider participating in an Internet program offering benefits such as free email, discounts, PCs, etc. in exchange for their personal information, 54% of Web users said it was somewhat possible or quite possible). The Privacy & American Business and Opinion Research Corporation has found that an "overwhelming majority of [Internet users] don't have a problem with companies collecting information on their buying habits and preferences" as long as they get something in return, such as customized offers and services. *Id.*

PCs, Web access, or customized services.[30] Many of the most successful Web sites, such as Hotmail, Ecircles, and Yahoo!, provide individuals with free services in exchange for information about the viewer and an opportunity to catch their eye with an advertisement.

Some business uses of personal information benefit consumers. The more a business knows about an individual, the better it can customize Web pages to meet her interests, develop targeted emails that provide her with useful information or discounts, and prevent credit card fraud in e-commerce transactions. For example, Ecircles uses the information its customers provide to remind them of their friends' birthdays.[31] Additionally, Ecircles sends its customers targeted advertisements that make it easier for them to buy gifts for their friends online.[32] Customized services and advertisements such as these make the Internet a more interactive and convenient medium for consumers.

However, recent incidents indicate that commercial uses of personal information are not always in the best interest of the consumer.[33] Geocities, a popular Web site, agreed to settle a claim that it had misrepresented to its customers why it was collecting personal information from them when they filled out an online membership application or registration form.[34]

---

30. *See* Brian L. Clark, *Are Free Offers Worth the Price?*, MONEY, Sept. 1999, at 170. More than half a million people have signed up since October 1998 to receive free Internet access in exchange for watching ads in the corner of their screen and giving businesses that advertise on the screen demographic information about themselves and their Web viewing habits. *See id.* Through Free-PC, individuals can get a free computer with Internet access if they answer questions about their hobbies, habits and families. *See id.* Yahoo! offers its customers a service called My Yahoo!, which allows users to set a customized homepage that features all of the new articles, stock quotes, and health tips they are interested in. In exchange, users give Yahoo! their name, zip code, information about their interests and all of the valuable marketing data that comes with knowing what news items a user considers most important and interesting. For more information, go to *My Yahoo!* (visited July 18, 2000) <http://my.yahoo.com>.

31. *See New and Cool at Ecircles* (visited July 15, 2000) <http://wwwd-00-02-ec.ecircles.com/templates/ec/x/news/index.html> (explaining many of the interactive uses and convenient features of the site).

32. *See id.*

33. *See* Liz Enbysk, *Ban All Online Profiles?* (Nov. 8, 1999) (visited April 16, 2000) <http://www.zdnet.com/anchordesk/story/story_4088.html>; Sara Robinson, *RealNetworks to Stop Collecting User Data*, N.Y. TIMES, Nov. 2, 1999, at C2. RealNetworks, a Web site that streams media technology on the Internet, was discovered secretly storing information about its users. It has recently agreed to stop this practice and to bring in a privacy expert to review its information uses. Another privacy abuse was committed by Liberty Financial, which had a young investors' site for children. The FTC reached a consent agreement with the company after it charged Liberty with falsely telling its customers that personal information collected from children on the young investors' site would be maintained anonymously. According to the agency, the financial and personal information Liberty collected about children and their parents was kept in an identifiable manner. *See* Rich Rojeck, *FTC Reprimands Liberty Over Kids' Web Site* (June 1, 1999) (visited April 16, 2000) <http://198.80.189.117/practice/management/compliance/19990601006.html>.

34. *See* In the Matter of Geocities, No. C-3850 (Feb. 12, 1999) (Complaint, paragrapbs 12-16; Final Decision and Order available at <http://www.ftc.gov/os/1999/9902/9823015d&o.htm> (visited July 15, 2000)).

Evidently, rather than using the information to benefit its customers with customization and better service, Geocities merely sold its customers' information to marketers for a profit.[35] The possibility of this type of abuse is significant considering that an FTC study found that ninety-two percent of all Web sites surveyed collected personal information.[36]

The information that businesses such as Geocities find so profitable to sell to other businesses[37] and to use for their own internal uses combines online and offline information about individuals. Businesses collect consumer information because current marketing theory teaches that if you understand the characteristics of individuals, you can find ways to make them loyal and profitable repeat customers.[38] On the Internet, businesses can gather information by "analyzing the raw traffic statistics and turning them into useful marketing data, like determining how many times the same people viewed an ad, how long they lingered and what route they took to get there."[39] Businesses can then combine Web site usage statistics with offline information about individuals' credit card purchase habits, travel arrangements, and monthly account balance to create valuable consumer profiles. A business can either use these profiles as a marketing tool or sell them to insurers, health care providers, credit card businesses, and

35. *See Geocities, supra* note 34. The FTC's power to police deceptive uses of consumer information on the Internet comes from its ability to bring enforcement actions under Section 5 of the Federal Trade Commission Act (FTCA). *See A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority* (Apr. 1998) (visited July 15, 2000) <http://www.ftc.gov/ogc/brfovrvw.htm>. This section is a basic consumer protection statute that provides that "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." 15 U.S.C. § 45(a)(1). The FTC can attack unfair or deceptive practices that occur on an industry-wide basis through administrative adjudication or trade regulation rules. If an organization were to violate the Children's Online Privacy Protection Act "with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule," it could be liable for civil penalities of up to $11,000 per violation. 15 U.S.C. § 45(a)(1).

36. *See* FTC REPORT, *supra* note 16, at 23 fig.1. According to the FTC, the Web sites they studied collected a "remarkable variety of personal information, including name, email address, postal address, telephone number, fax number, credit card number, Social Security number, age or date of birth, gender, education, occupation, income, hobbies, interests, and the type of hardware or software used by the online consumer." *Id.* at 24. Much of this information is collected from Internet users through surveys, Web site registration forms, cookies, and contest applications. *See id.* at 22-26.

37. *See* Kong, *supra* note 3 (noting that personal data is valuable in the digital economy and is being considered an asset of a company); Adam L. Penenberg, *The End of Privacy*, FORBES, Nov. 29, 1999, at 182 (stating that many banks, brokerages, and credit card issuers sell consumers' information to marketers); William Safire, *Nosy Parker Lives*, N.Y. TIMES, Sept. 23, 1999, at A29 (discussing the sale of personal information to third parties).

38. *See generally* DON PEPPERS & MARTHA ROGERS, THE ONE TO ONE FUTURE 18-50 (1993) (discussing how businesses can effectively market their items to the individual so that they become loyal and repeat customers).

39. Gandy, *supra* note 8, at 111 (citation omitted).

other commercial entities that may rely on this information to make decisions about their customers.[40]

Consumers are becoming more aware of the fact that businesses need their personal information for marketing purposes, revenue growth models, and as an extra source of income. Yet they are uncomfortable with this practice because businesses often do not give them enough information about how their data will be used.[41] Consumers deserve to know what third parties their information will be given to and how it will be used.

B. Individual Interests in Online Personal Information

It is undeniable that human beings need physical privacy,[42] but it is less clear why informational privacy is important to our daily existence. The West German Constitutional Court's 1983 decision, holding a Census Act unconstitutional, offers some insight into this issue. The Court reasoned that "[i]f someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu, and cannot estimate sufficiently the knowledge of parties to whom communication may possibly be made, he is crucially inhibited in his freedom to plan or to decide freely."[43] It is this connection between privacy and freedom that makes the loss of individuals' control over their personal information in George Orwell's novel *1984* so chilling.[44]

Each time we disclose information about ourselves to a chat line, in an online survey, or on a Web site registration form, we take the chance that such information will be used against us. This possibility is why Jeffrey Reiman, a privacy expert, considers privacy important. He recognizes that threats to our privacy pose a danger to our ability to engage

---

40. *See* Mulligan, *supra* note 4, at 2 (warning that one of the dangers of this practice is that the information collected about an individual "could be used to alter the prices at which goods or services, including important services such as life and health insurance are offered").

41. *See* Green, *supra* note 27 (stating that privacy policies explaining information practices are often hard to find and fail to accurately portray to consumers how data is tracked or used).

42. There are several philosophies regarding human beings' need for privacy. *See* DECKLE MCLEAN, PRIVACY AND ITS INVASION 71-90 (1995) (providing a general overview of what privacy gives human beings, including ethical standards, self-control, and emotional control through private moments); PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY (Ferdinand D. Schoeman ed., 1984) (compiling key essays on the value of privacy); FERDINAND D. SCHOEMAN, PRIVACY AND SOCIAL FREEDOM (1992) (arguing that in the context of social relations, privacy enables individuals to limit the amount of control society has over their lives). In simply discussing the concept of privacy, one must first determine whether one considers it to be a "state or condition, a desire, a claim, or a right." JAMES MICHAEL, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL AND COMPARATIVE STUDY 2 (1994). The concept of privacy is further complicated by the fact that what each society regards as "private" can vary widely. *See id.* For the purposes of this paper, I will limit my discussion to the human need for informational privacy.

43. Census Act Decision of the Federal Constitutional Court, Karlsruhe, Germany, *translated in* 5 HUMAN RIGHTS L.J. 94, 100.

44. GEORGE ORWELL, 1984 (1976) (illustrating the type of control an entity such as Big Brother can exercise over individuals when it knows everything about their lives).

freely in activities on the Internet.[45] Individuals falsify their personal information or do not participate in e-commerce at all in order to avoid a scenario in which their real world options are limited by the facts they divulged in cyberspace.[46] Individuals should not have to worry that a future employer or health care provider will make decisions about them based on the fact that when they were sixteen they were surfing Web sites about manic depression and suicide. In order to preserve freedom of action on the Internet, individuals must be granted basic privacy rights in regard to the use of their online personal information.

II

THE EFFECTIVENESS OF CURRENT PRIVACY PROTECTION SYSTEMS

As privacy becomes a more pervasive concern on the Internet, government regulators, privacy advocates, the general public, and businesses are working to develop solutions to protect online privacy. This Comment will discuss only three of the methods currently being used to protect privacy: government regulation, self-regulation, and technical solutions, focusing on one example of how each system functions. The critique of government regulation will focus on the Children's Online Privacy Protection Act; the discussion of self-regulation will evaluate privacy seal programs; and the analysis of technical solutions will concentrate on anonymizing software.[47] None of these techniques provides an adequate solution to serve the interests of businesses and individuals.

---

45. *See* Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 27, 37 (1995).

46. Unregulated corporate sharing of consumer information has led some Internet users to provide false information to Web sites. One privacy advocate promoted this practice by arguing that individuals should never give their true identity when signing up for something online. *See* Dan Fost, *Online Disguises from Prying Eyes*, S.F. CHRON., Sept. 23, 1999, at B1. *See also Center for Democracy and Technology Privacy Survey Graphs* (visited July 16, 2000) <http://www.cdt.org/privacy/survey/findings/results.html>.

47. Among the technical solutions currently being developed beyond anonymizing software are the Platform for Privacy Preferences (P3P) by the World Wide Web Consortium. P3P is a privacy enhancing technology (PET) which allows users to program their browsers to only interact with Web sites that meet their privacy preferences. *See* Joseph M. Reagle, Jr. & Rigo Wenning, *P3P and Privacy on the Web FAQ* (Apr. 18, 2000) on the World Wide Web Consortium Web site (visited July 15, 2000) <http://www.w3.org/P3P/P3FAQ.html>. The Internet Engineering Task Force (IETF) has suggested giving cookies greater privacy by creating a new version of the protocol and labeling cookies with privacy disclosures. *See* Daniel Jaye, *PICS extension for HTTP cookies* (visited July 15, 2000) <http://www.w3/org/PICS/extensions/cookieinfo-1_0.html>. Encryption technologies such as Pretty Good Privacy (PGP) have also been suggested as solutions to online privacy. For an example of a communications security Web site with an emphasis on PGP, see the Communications Security Web site (visited July 15, 2000) <http://www.commsec.com>.

A. *Government Regulation*

There are numerous laws and regulations in the United States governing the use of personal information in the private sector but they mainly focus on particular issues and often seek to address very specific problems.[48] The first federal rule to tackle the problem of privacy on the Internet is no exception. The Children's Online Privacy Protection Act[49] (COPPA) is designed to stop unfair and deceptive acts and practices involving the collection, or disclosure, of personal information from Internet users who are twelve and under.[50] Web sites lure children into buying items and giving information by using cartoon characters, games, and sweepstakes.[51] The fact that children are largely unaware of the privacy risks involved in revealing such information and that Web sites were actively collecting data from them spurred Congress to pass a bill that protects children.[52]

---

48. Among these laws, the most relevant are the Fair Credit Reporting Act, 15 U.S.C. §§ 1681, 1681(a) to 1681(t) (1968), *amended by* 15 U.S.C. §§ 1681(a)-1681(c), 1681(i), 1681(g), 1681(k), 1681(s) (1998), which requires credit agencies to allow consumers to review their credit records and check for inaccuracies; the Electronic Funds Transfer Act, 15 U.S.C. §§ 1601, 1693-1693(r) (1978), *amended by* 15 U.S.C. § 1693(b) (1996), which requires that institutions notify customers of third-party access to customer information on electronic fund transfers; the Cable Communications Policy Act of 1984, 47 U.S.C. § 631, *amended by* Pub. L. 98-549, § 1(a), 15 U.S.C. § 21; 18 U.S.C. § 2511; 46 U.S.C. §§ 484-487; 42 U.S.C. § 35; 50 U.S.C. § 1805 (1984), which provides privacy-related regulation of cable television service providers; the Video Privacy Protection Act, 18 U.S.C. §§ 2710-2711 (1988), which protects the privacy of consumers' video tape rental and sale records; and the Telecommunications Act of 1996, 15 U.S.C. § 79; 18 U.S.C. § 1462; 47 U.S.C. § 151 (1996), which includes provisions for protecting the privacy of "Customer Proprietary Network Information." *See generally* FRED H. CATE, PRIVACY IN THE INFORMATION AGE (1997) (providing an overview of the technologies threatening privacy and discussing the legal issues raised); DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES (1989) (containing a study of privacy legislation and regulatory systems in the U.S. and some European countries); PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW (1996) (proving a detailed study of the United States' privacy laws designed to protect data); ROBERT ELLIS SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (1992) (providing a summary of U.S. state and federal privacy laws).

49. Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, § 312.10, 112 Stat. 2681 (1998) [hereinafter COPPA]. On October 20, 1999, the FTC issued the final rules implementing COPPA. COPPA went into effect on April 21, 2000, and applies to personal information collected online from that date forward.

50. *See* Federal Register, Vol. 64, no. 212, Rules & Regulations, Nov. 3, 1999, 16 C.F.R. Part 312 at 59,888 (visited July 15, 2000) <http://www.ftc.gov/05/1999/9910/64fr5988.pdf>. Marketing products directly to children over the Internet has been a concern, especially with the advent of new commerce systems such as "iCanbuy," which allows children to create lists of the items they want to buy and keep bank accounts with money that they can draw upon to make online purchases. *See* Joe Salkowski, *Privacy-Protection Policy For Kids Can Benefit Adults,* CHI. TRIB., Nov. 1, 1999, § 4, at 2; Bob Thompson, *The Selling of the Clickerati,* WASH. POST, Oct. 24, 1999 (Magazine), at 11.

51. *See* Thompson, *supra* note 50.

52. Senator Bryan, a sponsor of the legislation, stated that the goals of the legislation are:

> (1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of personally identifiable information of children collected online;

The type of privacy protection that COPPA has extended to children also should be developed for adults, who currently have no protection against the collection of their personal information on the Internet. However, COPPA is not the ideal model for the protection of individuals' online privacy even though it meets several of the goals set out in the Introduction. The Act satisfies the Choice objective (goal #1) by requiring parental permission before a site can collect a child's personal information. In accordance with the Enforcement and Redress objective, the law provides for the enforcement of these regulations (goal #6).[53] The Act therefore includes mechanisms for controlling access to personal information and enforcing its proper use.

However, COPPA still fails to adequately meet the needs of consumers. COPPA requires that Web sites obtain a parent's address and name so that they can send them a consent form. To verify that the parent is the one who has denied or given consent, some Web sites may choose to require credit card numbers or photocopies of driver's licenses. The process of giving consent therefore may pose a privacy risk in itself. The consent provision also makes the Act fairly cumbersome for parents to use because it requires that they fill out a form each time their child logs on to a site collecting information. It therefore fails to meet the fifth objective of an effective privacy system—Ease of Use.

COPPA's narrow focus exemplifies this country's tendency to react to privacy problems rather than anticipate problems and develop solutions to them.[54] In contrast to the United States, Europe has taken a comprehensive approach to privacy, as evidenced by its passage of the European Union (E.U.) Data Protection Directive.[55] The E.U. Directive establishes a reliable and clear regulatory framework that ensures a high level of protection for the privacy of individuals' information throughout the European Union. It requires all entities that collect, hold or transmit personal information within the E.U. to do so only for specific, explicit, and legitimate

---

and (4) to protect children's privacy by limiting the collection of personal information from children without parental consent.

144 CONG. REC. S11,657 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan).

53. The FTC is empowered to implement and enforce COPPA by its section 5 jurisdiction. In addition, section 6504 of COPPA authorizes state attorney generals to enforce compliance with the final rule by filing actions in federal court after giving the FTC prior written notice. Another enforcement procedure is found in the safe harbor rules that subject participants to a yearly audit of their information practices. *See* COPPA, *supra* note 49. As stated earlier, the FTC's promotion of self-regulation for privacy protections on the Internet makes frequent and effective use of this power unlikely. *See* FTC, *Self-Regulation and Privacy Online*, *supra* note 35.

54. *See* Reidenberg, *supra* note 28 at 772 ("For years, the United States has relied on narrow, ad hoc legal rights enacted in response to particluar scandals involving abusive information practices. The approach has led to incoherence and significant gaps in the protection of citizens' privacy.").

55. European Union Data Protection Directive 95/46/EC, OFFICIAL JOURNAL OF THE EUROPEAN COMMUNITIES, No. L. 281, Nov. 23 1995. The unofficial version can be found on the Europa Web site (visited July 17, 2000) <http://europa.eu.int/eur-lex/en/lif/dat/1995/en-395L0046.html>.

purposes.[56] These basic requirements help to eliminate privacy abuses, such as the buying and selling of sensitive information, while facilitating consumer confidence and commercial compliance with privacy principles.

As a result of our current ad hoc privacy legislation, American consumers are hesitant to participate in e-commerce. In order to improve privacy protections in this country the United States should adopt a comprehensive approach similar to that used by the European Union. American businesses will need to adopt this approach, even if it is not required by the U.S. government, in order to conduct e-commerce with consumers in E.U. countries.[57]

B. Self-Regulation

A recent privacy poll suggests that consumers may be more likely to provide sensitive information to a Web site with a posted privacy policy or a seal of approval from a trusted organization such as Good Housekeeping.[58] However, the presence of a posted privacy policy can actually provide consumers with a false sense of security.[59] A report by

---

56. *See id.* at Article (a)(1)(a).

57. To expand e-commerce to Europe, American companies are going to have to adhere to stronger privacy policies in order to comply with the European Union Data Protection Directive. The Directive states that data transfers to countries outside of the E.U. may only take place if the third country ensures an "adequate level of protection." E.U. Data Directive, Articles 25-26; *see also* CULLEN INTERNATIONAL, A BUSINESS GUIDE TO CHANGES IN EUROPEAN DATA PROTECTION LEGISLATION 14-15 (1998); PETER P. SWIRE AND ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE AND THE EUROPEAN PRIVACY DIRECTIVE (1998) (providing a complete discussion of the E.U. Data Protection Directive and its implications for commerce between Europe and the United States); Emma Tucker, *Deadlock in US-EU Talks on Data Law*, FIN. TIMES, Oct. 8, 1998, at 6 (noting that the E.U. could stop exports in personal information to the U.S. if the country does not come up with adequate protections). At the time of publication, the U.S. and E.U. had agreed on a safe harbor to the E.U. Directive which would allow American businesses which adhere to its principles to receive data transfer from European countries. *See Commerce Secretary William M. Daley Hails U.S.-EU "Safe Harbor" Privacy Arrangement* (Mar. 14, 2000) (visited Apr. 15, 2000) <http://204.193.246.62/public.nsf/docs/8B7937D138B4F735852568A30053A385> (noting that the U.S. Department of Commerce and the E.U. have "reached an arrangement on a safe harbor system which will allow continuing data flows between the U.S. and the EU and ensure privacy protection for EU citizens' personal information").

58. *See generally* Lorrie Faith Cranor et al., *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy* (Apr. 14, 1999) (visited July 15, 2000) <http://www.research.att.com/library/trs/TRs/99/99.4/99.4.3/report.htm> (noting that 28% of consumers surveyed said that they would be more likely to provide information such as their name and address if the site they were using had a privacy policy, and 58% said they would be more likely to provide it if the site had both a privacy policy and a seal of approval from a well-known organization such as the Better Business Bureau or the American Automobile Association). The survey results were based on the analysis of 381 questionnaires completed between November 6 and November 13, 1998 by American Internet users. *See id.*

59. In my own research, I found privacy policies tended to benefit businesses more than consumers. For example, the Nike Web site privacy policy assures its users that Nike only uses the information they provide "to better know our visitors and possibly tailor any specific features, promotions, or other notifications to you." *Nike* (visited Sept. 28, 1999) <http://www.nike/com>. Nike

Forrester Research found that ninety percent of Web sites fail to comply with basic privacy policies.[60] Additionally, many sites create deceptive privacy policies that "use vague terms and legalese that serve to protect businesses and not individuals."[61] As a result, few consumers actually read posted privacy policies, and even fewer actually understand them.[62]

Privacy seal programs are one attempt to resolve this problem. These programs provide consumers with an easy way to evaluate a site's privacy policy and determine whether a Web site is using the personal information it collects in ways that offend them.[63] Seal programs require their licensees "to abide by codes of online information practices and to submit to various types of compliance monitoring in order to display a privacy seal on their Web sites."[64] When a consumer sees a seal on a Web site, she knows that the site follows a basic set of privacy rules.

TRUSTe is one such program.[65] To earn and maintain a TRUSTe seal, a business must follow TRUSTe's standards for notice, choice, access, and security that are based on guidelines set by the Online Privacy Alliance (OPA), a cross-industry coalition of more than seventy global companies

---

gives visitors a choice as to whether or not they want to receive mailings and special offers from the company. The privacy policy seems fair until the following statement: "However, this data in an aggregate form may be provided to other parties for marketing, advertising, or other uses." *Id.* The consumer should be told to which "other parties" Nike gives the information and what "other uses" they may employ.

Coca-Cola's site has some interesting disclaimers in its privacy policy as well. It states that

> [a]ny communication or material you transmit to the Site by electronic mail or otherwise, including any data, questions, comments, suggestions or the like is, and will be treated as, non-confidential and nonproprietary. Anything you transmit or post becomes the property of The Coca-Cola Company or its affiliates and may be used for any purpose, including, but not limited to, reproduction, disclosure, transmission, publication, broadcast and posting. Futhermore, The Coca-Cola Company is free to use any ideas, concepts, know-how, or techniques contained in any communication you send to the Site for any purpose whatsoever including, but not limited to, developing, manufacturing and marketing products using such information.

See The Fine Print (visited Sept. 28, 1999) <http://www.coke.com/legal.html>. The legal practices of the Nike and Coca Cola Web sites indicate to me that self-regulation is not enough to provide consumers with control over the use and dissemination of their personal information. *See also* text accompanying *infra* note 60.

60. *See* Dembeck, *supra* note 20.

61. *Id.*

62. Considering the length and complexity of many posted privacy policies, it would be difficult for a nser to fully read and understand the policy of every Web site they click on. For example, Yahoo!'s privacy policy is ten pages long. *See Privacy Policy* (visited July 15, 2000) <http://docs.yahoo.com/info/privacy/>.

63. TRUSTe defines "personally identifiable information" as "any information that can be used to identify, contact, or locate a person, including information that may be linked with identifiable information from other sources, or from which other personally identifiable information can easily be derived." FTC, *Self-Regulation and Privacy Online*, *supra* note 35, at 10 n.48.

64. *Id.* at 9.

65. *See TRUSTe* (visited July 15, 2000) <http://www.truste.org>.

and associations concerned with Internet privacy.[66] Programs like TRUSTe meet the first three goals (Choice, Notification, and Verification) by ensuring that individuals have the right to make decisions about their information and are aware of who has their information, how it is used,[67] and whether a site is following the privacy policies they have set out. Seal programs ensure a site's compliance with program requirements by instituting third-party monitoring and periodic reviews of licensees' information practices.

While privacy seal programs have helped to promote fair information collection on the Internet,[68] they alone cannot resolve the privacy problem. The privacy seal system is not uniform across the Internet and will most likely never be. For example, TRUSTe has a thousand licensees and BBBonline, auother privacy seal program, has only four hundred sites posting their seal.[69] If a consumer were to rely solely on seal programs to protect her privacy, her access to the World Wide Web would be limited to a maximum of 1,400 sites.[70] Unless these programs are able to aggressively push their product to the Internet community they will be unable to keep up with the exponential growth of cyberspace.[71]

Ironically, if the privacy seal producers convince a larger portion of the Internet community to sign on to their systems, they may be less effective in regulating these sites' privacy policies. Seal programs will not be able to closely evaluate every Web site's privacy policies when there are

66. For more information on the Online Privacy Alliance, see the organization's Web site (visited July 16, 2000) <http://www.privacyalliance.org>.

67. TRUSTe achieves this by only awarding privacy seals to sites that adhere to the organization's "program principles" of disclosure, choice, access, and security. *The TRUSTe Program Principles* (visited July 16, 2000) <http://www.truste.org/webpublishers/pub_principles.html>. Web sites also agree to comply with ongoing TRUSTe oversight and their alternative dispute resolution process. For more information, see *id.*

68. *See TRUSTe Testifies Before House Judiciary Committee* (May 27, 1999) (visited July 16, 2000) <http://www.truste.org/about/about_committee.html> (stating that TRUSTe has helped to promote fair information collection and use practices online).

69. *See TRUSTe Approves 1000th Licence* (visited July 16, 2000) <http://www.truste.org/about/about_1000th.html> (announeing that TRUSTe approved its 1000th Web site as of January 2000); *Reliability Program Participants* (visited Apr. 2, 2000) <http://www.bbbonline.org/databases/search/list.cfm> (identifying BBBonline licensees as of March 25, 2000).

70. This assumes that a consumer would only use sites with either the TRUSTe or BBBonline seals. There are other seal programs such as CPA Web trust (19 sites post the seal), but since TRUSTe and BBBonline are the most widely known seal programs, the number of sites monitored by additional seal programs is probably low.

71. Seal programs would most likely respond to this concern by arguing that their programs will spread because sites will find that the seal improves their customer relations and business. *See TRUSTe's Privacy Program Bolsters Consumer Trust* (visited July 16, 2000) <http://www.truste.org/newsletter/winter97.html#05> (stating that privacy seals give businesses credibility with consumers). However, this argument only takes into account the good actors and does not recognize the fact that sites which profit from the sale of consumers' information will not be motivated by consumer relations to change their privacy policies.

millions, rather than thousands, of customers signing up for their service. Thus, while the number of sites approved by TRUSTe and BBBOnline go up, the quality of the privacy policies these organizations endorse may go down. In addition to these problems, there is the danger that Web sites will post counterfeit seals in order to get consumers to provide them with information.[72] Without comprehensive laws prohibiting privacy abuses, seal programs will remain a limited solution to online privacy.

C. *Technological Solutions*

Anonymity refers to the absence of identifying data in a transaction—the identity of a party cannot be extracted from the data itself or by combining the transaction with other information. Technologies such as those used by Anonymizer allow users to surf the Internet anonymously.[73] When viewing the Internet this way, a user's identity is masked and any cookies she creates are deflected.[74]

Anonymizing systems may provide individuals with the right to be "let alone," but they fail to promote beneficial exchanges of information. Anonymizing systems meet the goals of Choice (goal #1) and Ease of Use (goal #5) because they readily allow an individual to control access to her personal information. However, an anonymous consumer may encounter situations where she will have to disclose her personal information in order to get a desired benefit, such as customization, a free service, or acceptance into a Web site's club membership. In these situations, technological solutions do not continue to protect a consumer's identity when she chooses to purchase items, register for benefits such as customization, or fill out online surveys. Anonymizing programs are inadequate because they do not give individuals the ability to control uses of their personal information beyond non-disclosure; they do not require that consumers be informed of who receives the information that they choose to disclose; and they do not provide a means for verifying that proper information practices are followed by a Web site. Anonymous surfing therefore does not offer individuals enough choices: they must either surf anonymously, without the benefits of free services and customization, or provide information to a Web site, giving up the ability to control the use or dissemination of the

72. The TRUSTe response to this issue can be found at *Frequently Asked Questions* (visited July 16, 2000) <http://www.truste.org/users/users_faqs.html#pirate>. TRUSTe asserts that a trustmark's authenticity can be verified in several ways although it does admit that there is no "100 percent guarantee" that the TRUSTe seal will not be pirated.

73. *See Anonymizer* (visited July 16, 2000) <http://www.anonymizer.com>.

74. Other businesses with similar products include Junkbusters, which works between the browser and the Internet to throw out cookies and other information that a user does not want to reveal. *See Junkbusters* (visited July 16, 2000) <http://www.junkbusters.com>. Web Incognito from Privada even compartmentalizes and encrypts information so that no one can make a connection between your Web identity, the name, password and personal data you give to a Web site, and your real world identity. *See Privada* (visited July 16, 2000) <http://www.privada.net>.

information they provide. An effective privacy system should provide consumers with both the right to control their information and the ability to receive benefits.

Anonymizing software also fails to meet the needs of businesses. Because anonymous surfing devices eliminate pseudo-anonymous trackers such as cookies and mask individuals' identities, commercial Web sites are unable to get the type of marketing information they need from consumers to continue providing free services.

III
A LICENSING SYSTEM SOLUTION

A. The Superiority of Licensing

Licensing is a contractual system based on the exchange of commodities that gives the contracting parties the right to determine the terms of the contract.[75] A licensing system would allow an Internet user (licensor) greater control over what an Internet business (licensee) does with her personal information. She would retain ownership of her information and would only grant a company revocable permission to use it. If a consumer were to sell her information, she could only do so once, because she would be passing her property rights over to the business. However, by licensing her information, a consumer can control which businesses have access to her information, how businesses use it, and what form of compensation she should receive. In a licensing agreement, an individual could specify whether the information she provides can be further sold to a third party and if it is, what benefit she would require for this use. If the licensee failed to follow the terms of the agreement, an individual could revoke the license. Additionally, individuals could control the type of information a business has about them by choosing which businesses to grant a license to and what information to share with each one. For example, a licensing agreement might read:

> Company *X* is authorized to collect my name, address, income, and online buying habits. It may use this information to determine what products I will be most interested in buying, to make decisions about its own product development, and to send me emails about changes to this product. I grant Company *X* the right to distribute my name only to third parties with privacy policies equal to Company *X*'s until 1/1/02 and I will receive $2.00 each time my name is transferred to such a third party. After 1/1/02, Company *X* must cease all use of this information and will no longer have any rights or interest in it.

75. *See generally* Gregory J. Battersky & Charles W. Grimes, LICENCING DESK BOOK 3-4 (1999).

Such a license makes explicit the licensor's rights and the licensee's terms of use. Thus, licensing is an effective method for protecting privacy while allowing for the beneficial use of Internet generated information.

B. *Property Rights in Personal Information*

A licensing system cannot function unless consumers have a property right to information about themselves.[76] Recognizing a property right in such information would not only give consumers certain privileges, but also would give businesses a legal incentive to pay consumers for the use of their personal information. Without such an incentive businesses could continue collecting, using, and disseminating consumers' information with little regard for consumers' interests. Under current law, "the ownership right to personal information is given to the collector of that information, and not to the individual to whom the information refers."[77] Unless individuals are given property rights in the information they create, businesses will argue that they own the information generated and collected on their Web sites.

There is disagreement among legal commentators and individuals in the privacy community, however, as to whether or not there should be property rights in personal information.[78] Some have argued that individuals should have a property right in their personal information.[79] Others have argued from the economic perspective that propertizing information to protect privacy creates restrictions that "inhibit decisionmaking, increase transaction costs, and encourage fraud."[80] In American law, the traditional

---

76. Giving individuals property rights in their information would give them "the rights guaranteed in the fair information practices guidelines: the right to be informed of data collection and transfer; the right to limit data collection, data transfers, and secondary uses; the right to access one's personal data and make corrections; and the right to have one's personal data maintained securely." Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1196 (1997).

77. Kenneth C. Laudon, *Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information in* U.S. DEP'T OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997) (visited April 5, 2000) <http:www.ntia.doc.gov/reports/privacy/selfreg1.htm#1D>.

78. *See* Pamela Samuelson, Privacy As Intellectual Property (on file with author) (diseussing in-depth the propertization of personal information and its implieations for privacy).

79. *See, e.g.*, ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? 180-83 (1994); WESTIN, *supra* note 8, at 324 (arguing that "personal information, thought of as the right of decision over one's private personality, should be defined as a property right"); Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56 (1999); Patrieia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 10 (1992); Carl Shapiro & Hal Varian, *US Government Information Policy* (visited May 28, 1997) <http://www.sims.berkeley.edu/~hal/papers/policy.pdf>.

80. Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L. J. 2381, 2382 (1996) (citing to Symposium, *The Law and Economics of Privacy*, 9 J. LEGAL STUD. 621 (1980)).

view "has been that information cannot be owned by any person."[81] The Supreme Court's finding that information is private property in *Ruckelshaus v. Monsanto Company*[82] and *Carpenter v. United States*[83] suggests, however, that the Court might be willing to consider the concept of a property right in personal information.[84]

It is important to ask in this discussion whether the propertization, and thus the commodification of personal information, is a good thing,[85] and what the extent of such a property right would be. Another consideration is whether information actually can be controlled and how people will keep track of every piece of information they create in the online and offline worlds. Finally, one must consider the transaction costs involved in making each individual's information a property right that companies would have to pay to use. For instance, there is a great deal of information about people already in the marketplace (such as their names, addresses, phone numbers). Therefore, any new system would need to address how to provide people with exclusive access to such information and control over its dissemination from that point forward. I raise these issues because I think they are important to consider when evaluating a licensing system. Nevertheless, a detailed discussion of these compelling matters is beyond the scope of this Comment.

C. *Problems That Could Arise Under A Licensing System*

A licensing system presents several potential problems. First, businesses could choose to deal only with consumers who are willing to license their personal information. This option would be unlikely if only a few people decided to license their information. However, if the vast majority chose to participate in this system, then privacy holdouts might find themselves with restricted access on the Internet because businesses would be in a position to refuse to deal with consumers who do not license their information.

A licensing system also may breed incentive structures that will limit consumers' options and control over their personal information. Businesses may make benefits so attractive that the vast majority of their consumers

81. Samuelson, *supra* note 78, at 5 (citing *Feist Pub., Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340 (1991)).

82. 467 U.S. 986 (1984) (holding that research data given to a federal agency could be considered "property" within the meaning of the Fifth Amendment of the Constitution).

83. 484 U.S. 19 (1987) (holding that a reporter's personal knowledge of the publication schedule and contents of his newspaper column constituted the "property" of the publisher).

84. *See* Pamela Samuelson, *Information as Property: Do* Ruckelshaus *and* Carpenter *Signal a Changing Direction in Intellectual Property Law?*, 38 CATH. U. L. REV. 365 (1989) (critiquing the *Ruckelshuas* and *Carpenter* opinions and suggesting that we should carefully consider the consequences of classifying information as property).

85. *See* Samuelson, *supra* note 84, at 10-18; *infra* Part V.B.

decide to share even their most sensitive information. This scenario might proceed as follows:

> *A* gives a license to Company *B* to use all of her banking information for any purpose for the next ten years in exchange for an ATM fee of five cents per transaction. In contrast, *C* gives a license to Company *B* to look at her daily bank balance, but not her daily checking transactions. Because *C* divulges less information than *A*, the company may refuse to provide banking services for her unless she agrees to pay one dollar per ATM transaction. Finally, a customer who does not license any information to Company *B* at all might find herself required to pay three dollars per ATM transaction.

This hypothetical suggests businesses may use their economic strength to create incentive structures that force the consumer to share their personal information in order to save money.[86]

A licensing system potentially could become a cumbersome process for consumers. Individuals might have to make an agreement with every Web site they log on to. It is unrealistic to assume that Internet users would want to take the time to develop and negotiate a separate licensing agreement each time they visit a new site. However, this problem is being addressed by businesses, such as Lumeria, that are working to establish themselves as trusted infomediaries who will negotiate information transactions between consumers and commercial entities.[87] Infomediaries have been described as brokers for both consumers and vendors.[88] For the consumer, the infomediary is a trusted agent that learns her interests and habits and evaluates agreements with vendors based on this knowledge.[89] For businesses, the infomediary offers insight into consumer behavior that helps them reach their targeted market more efficiently and cheaply.[90]

A licensing system might not provide enough incentives for businesses to contract with individuals for use of their personal information. Many businesses have been collecting and storing information about

---

86. This hypothetical ignores the possibility of competitors who may be willing to take less information from their customers while still offering low ATM transaction fees. Given the relative lack of competition in banking services, however, this might not be an inappropriate omission.

87. *See Lumeria* (visited July 16, 2000) <http://www.lumeria.com>. *See also infra* Part IV.B (discussing electronic agents).

88. *See* JOHN HAGEL III & MARC SINGER, NET WORTH 19-20, 24-26, 40-48 (1999); *see also* John Hagel III & Jeffrey F. Rayport, *The Coming Battle for Customer Information*, HARV. BUS. REV., Jan.-Feb. 1997, at 53. This system recognizes that "consumers won't have the time, the patience, or the ability to work out the best deals with information buyers on their own. In order to help them strike the best bargain with vendors, new intermediaries will emerge. They will aggregate consumers and negotiate on their behalf within the economic definition of privacy determined by their clients." *Id.* at 60.

89. *See* HAGEL & SINGER, *supra* note 88, at 30-34. As the authors point out, the challenge for the infomediary will be in gaining consumers' trust and assuring them that their profiles will be protected.

90. *See id.* at 42-48.

consumers from offline and online sources for many years.[91] They will argue that they own the marketing lists and databases they have developed as well as the information in them. Why should they pay for information they already own? If businesses continue to sell the information they have without permission, individuals are put at a disadvantage. One benefit consumers have in this situation is that the information businesses now possess will quickly become outdated; when a licensing system takes effect, businesses will no longer be able to obtain an individual's changing Web site viewing patterns, registration information, survey results, marital status, income, address, or telephone number without a contractual agreement. In a fast-paced marketplace such as the Internet, having outdated information can be deadly for any business that bases its marketing, financing, product development, or growth patterns on consumer information. This feature of the Internet gives consumers an advantage and suggests that a licensing system for information might work.

Finally, some Web sites may not have the resources or incentives to contract with individuals for information. If infomediaries prohibit consumer access to Web sites that have not accepted their standardized agreement, some Web sites will be denied their user base. This is particularly troubling because one of the virtues of the Internet exists in the access it provides to businesses and organizations with fewer resources. Since most infomediaries are still in the development stage, they have not yet addressed this issue. This problem may be resolved by having a pop-up screen that would tell a user that a site will not make an agreement with her. The user would then have the choice of waiving her right to make a contract and logging on to the site or exiting the page. Consumers therefore will have to weigh the value of their privacy against the value of the information or service they are seeking.[92]

A licensing system allows individuals to determine which businesses have access to their personal information and how it is used by giving them the right to refuse to license their information to a business with whose practices or third party uses they do not agree. Infomediaries such as Lumeria could eliminate any cumbersome problems with the licensing system by making decisions about what terms should apply to each Web site with which an individual contracts, evaluating the costs and benefits, closing the deal, and collecting the benefits or monetary compensation. However, one unresolved problem with a licensing system is that it might not provide consumers with a way to verify that a Web site is complying with the terms of the agreement. This is a service that an infomediary will have to offer to succeed in the marketplace. Companies such as Lumeria

91. *See supra* notes 1-4.

92. Users currently make this choice each time they log on to a site such as Coke.com, in which every piece of information is owned by the site. *See supra* note 59.

could eventually enter into partnerships with online seal programs to resolve this problem. Seal programs like TRUSTe could use their existing auditing systems, combined with market pressure, to catch companies that violate their licenses, and encourage good business practices.

IV
IMPLEMENTATION OF A PERSONAL INFORMATION LICENSING SYSTEM UNDER UCITA

In order for a licensing system to work there must be a legal framework supporting it. Uniform adoption of a licensing system among domestic Web sites could become a legal requirement with the adoption of UCITA by all fifty states. The Act was originally drafted as part of Article 2 of the Uniform Commercial Code (U.C.C.) in order to standardize transactions involving licenses of information and software in electronic and other digital based commerce.[93] In July of 1999, UCITA[94] was adopted by the National Conference of Commissioners on Uniform State Laws (NCCUSL).[95]

This Part will demonstrate how individuals can use UCITA to protect their online privacy. While one of the goals of UCITA is to "clarify contract law premises and to facilitate electronic and other digital-based commerce," the Act was written with the needs and concerns of the software industry in mind.[96] However, this Part will argue that UCITA applies to licenses of personal information and will show how it would facilitate a licensing system.[97]

---

93. *See generally* Robert W. Gomulkiewicz, *The License is the Product: Comments on the Promise of Article 2B for Software and Information Licensing*, 13 BERKELEY TECH. L.J. 891 (1998) (providing an understanding of the purpose and history of Article 2B while critically discussing its ability to meet the author's objections); Lawrence Lessig, *Sign It and Weep* (Nov. 20, 1998) (visited July 15, 2000) <http://www.thestandard.com/article/display/0,1151,2583,00.html> (discussing the objectives of Article 2B while evaluating its practicality).

94. *See* UNIF. COMPUTER INFO. TRANSACTIONS ACT (Draft, July 1999).

95. The passage of UCITA caused many academics, journalists, and lawyers to raise red flags in alarm over its implementation and effectiveness. *See, e.g.*, Maureen A. O'Rourke, *Progressing Towards a Uniform Commercial Code for Electronic Commerce or Racing Towards Nonuniformity?*, 14 BERKELEY TECH. L.J. 635 (1999); Hiawatha Bray, *Stop Hardline on Software*, SAN ANTONIO EXPRESS-NEWS, Aug. 29, 1999, at 4J; Ed Foster, *The Gripe Line: Beware of Licensing Terms Giving Vendors the Right to Detonate Software Bombs*, INFOWORLD, Aug. 30, 1999, at 81; Rosalind C. Truitt, *Info Licensing Act Opposed*, PRESSTIME, Sept. 1999, at 16. This Comment sidesteps these criticisms of UCITA to consider how we can actually work with this law once it is passed. While UCITA may have some negative consequences for software buyers, it also may provide all consumers with an effective way to protect their privacy on the Internet.

96. Raymond T. Nimmer, *Breaking Barriers: The Relation Between Contract and Intellectual Property Law*, 13 BERKELEY TECH. L.J 827, 829 (1998).

97. For a discussion of other applications of UCITA outside of the software realm, see Jane C. Ginsburg, *Authors as "Licensors" of "Information Rights" Under U.C.C. Article 2B*, 13 BERKELEY TECH. L.J. 945 (1998) (providing an analysis of several sections of U.C.C. Article 2B and their relevance to protecting authors' copyrighted works).

A. *Personal Information Transmitted Over the Internet Falls Within the Scope of UCITA*

UCITA was designed to standardize licensing practices for software. Section 103(a) states that "[t]his [Act] applies to computer information transactions."[98] Section 102(12) defines a "computer information transaction" as "an agreement . . . to create, modify, transfer, or license computer information or informational rights in computer information."[99]

"Computer information" is defined in section 102(11) as "information . . . that is in digital or equivalent form capable of being processed by a computer."[100] Because any information an individual gives or creates while on the Internet is transferred into digital form as it travels over the network, personal information should easily fall within this definition. However, the definition of "computer information" may not extend such broad-blanket protection because personal information may not be considered "information."

Section 102(37) defines "information" as "data, text, images, sounds, mask works, or computer programs, including collections or compilations thereof."[101] Personal information fits best under the term "data." "Data" is not defined in the final version of the Act, but the July 1999 draft refers to it as "facts whether or not organized or interpreted."[102] This definition is consistent with the names, addresses, digital recording of hits to different Web sites, and personal preferences that constitute a consumer's personal information. Thus, personal information transmitted over the Internet is "data," and therefore falls within the definition of "information."

The language of the Act seems to support the inference that personal information sent over the Internet is the type of "information" included within the definition of "computer information" because that information is in "electronic form" and "obtained from or through the use of a computer."[103] From this conclusion, it seems easy to assume that sending personal information over the Internet should be considered a "computer information transaction" protected by the Act.

However, the legislative history of UCITA does not support this interpretation. The July 1999 draft of the Act narrows the scope of a "computer information transaction" by asserting that

---

98. UNIF. COMPUTER INFO. TRANSACTIONS ACT § 103(a) (Draft, July 1999).
99. *Id.* § 102(12).
100. *Id.* § 102(11).
101. *Id.* § 102(37).
102. *Id.* § 102 reporter's notes 22.
103. Section 102(11) of UCITA defines computer information as "information in electronic form that is obtained from or through the use of a computer, or that is in digital or equivalent form capable of being processed by a computer. The term includes a copy of information in that form and any documentation or packaging associated with the copy." *Id.* § 102(11).

> [t]he mere fact that information related to a transaction is sent or recorded in digital form is not sufficient to be within this definition. The creating, modifying or obtaining [of] the computer information itself must be a primary purpose of the agreement. Thus, a contract for airplane transportation is not a transaction within this Act simply because the ticket is in digital form. The subject matter is not the computer information, but the service—air transportation from one location to another.[104]

The NCCUSL draft of UCITA states that the "obtaining [of] computer information itself must be a primary purpose of the agreement."[105] This leads to the question of whether the subject matter of the transaction is determined from the buyer's or the seller's perspective. The Act seems to contemplate transactions involving the movement of information in one direction rather than two. Possibly this confusion could be resolved by viewing each exchange as a separate transaction. Therefore, unlike in the airplane ticket example, if a consumer sent her information in digital form to a company that would be a transaction whose primary purpose was obtainment of "computer information." In a licensing agreement for an individual's personal information, the subject matter of half the transaction is the electronic information being transmitted. The subject of the other half of the transaction is the "price" to be paid for that information. This "price" could be money, information or customized benefits. And, if these items were exchanged with the consumer via the Internet, they could be considered to be in digital form.

The drafters also restricted the types of "computer transactions" covered by UCITA. The Reporter's Notes state that "a transaction is not for the creation of computer information in the sense intended here where the contracted-for activities are merely secretarial or clerical in nature. The computer information must be produced through some business, professional, artistic, or imaginative effort."[106]

The fact that our interaction with the Internet is never the same each time we log on is a reflection of the originality of our online actions and the different experiences each of us create in cyberspace. One could argue therefore that information about consumers' hobbies, their discussions on chat lines, and their answers to surveys should be considered "imaginative" efforts because they are unique ideas of an individual.[107] This line of reasoning is tenuous and would most likely not hold up under scrutiny by the courts. Individuals could therefore attempt to contract around this

104. *Id.* § 102 reporter's notes 7 (Draft, July 1999).

105. *Id.*

106. *Id.*

107. Imaginative is defined as "created by, indicative of, or marked by imagination or creativity"; imagination is defined as "such power of the mind used creatively"; creative is defined as "marked by originality." WEBSTER'S II NEW COLLEGE DICTIONARY 551 (1995).

limitation by stating in the agreement that "personal information, Web usage information, and any other data generated or provided by the individual is considered to be created through a 'business effort' for the purposes of this agreement." Still, the NCCUSL draft and the current text of UCITA leaves this an unresolved issue which warrants further consideration and research.

B. The Benefits of Licensing Personal Information Under UCITA

This Section will show how UCITA benefits information licensors and it will discuss how electronic agents can be used under UCITA to simplify contract formation. It then will evaluate specific language in UCITA to highlight terms in the Act that benefit licensors. Finally, it will consider how UCITA can protect commercial entities.

1. The Use Of Electronic Agents For The Creation Of Contracts In Personal Information

A potentially problematic aspect of a licensing system is that it may be cumbersome. Consumers may quickly become frustrated and abandon the system if they have to take the time to create a contract with every Web site they log on to. This problem can be solved technologically through the use of electronic agents, such as Lumeria, that automatically negotiate and complete contracts. While current contract law does not allow for the creation of contracts via electronic agents, UCITA does.[108]

An electronic agent, rather than the consumer, will review the privacy policy of each Web site an individual visits and settle on a standard agreement. Businesses also will be able to have their own infomediaries enter licensing agreements on their behalf, thereby lowering their transaction costs.[109] Electronic agents may be more meticulous negotiators than

---

108. Section 202(a) states that "[a] contract may be formed in any manner sufficient to show agreement, including offer and acceptance or conduct of both parties or operations of electronic agents which recognize the existence of a contract." UNIF. COMPUTER INFO. TRANSACTIONS ACT § 202(a) (Draft, July 1999); *see also id.* § 102 reporter's notes 18 (defining an "electronic agent" as

> an automated means for making or performing contracts. The agent must act independently. Thus, mere use of an automated means such as a telephone or e-mail system does not entail use of an electronic agent. The term includes a computer program, but is not limited to that technology. The automated system must have been selected, programmed or otherwise used for that purpose by the person to be bound by its operations.)

109. UCITA allows for contracts to be formed between two electronic agents. *See id.* § 206(a) ("A contract may be formed by the interaction of electronic agents. If the interaction results in the electronic agents engaging in operations that confirm or indicate the existence of a contract by commencing performance, a contract is formed unless the operations resulted from fraud, electronic mistake, or the like."). Consumers and businesses will both have to be aware that under section 107 they are "bound by the operations of the electronic agent, even if no individual was aware of or reviewed the agent's operations or the results of the operations." *Id.* § 107(d). Thus, while the use of electronic agents will save time, it could lead to further problems such as confusion over offer and acceptance, unfavorable terms for one of the parties, or the formation of contracts that include terms to which one party did not agree. On the other hand, many consumers do not even fully read the contracts

individuals themselves. Thus, as the use of electronic agents become more common, consumers may find that they are fairly effective contracting tools that save time and a tremendous amount of work.

2. *UCITA May Help Consumers Obtain Favorable Licensing Terms*

UCITA may reduce some of the inequalities of bargaining power that arise between contract parties by setting default terms that consumers or their electronic agents might be unable to negotiate themselves. While consumers do have a valuable commodity to exchange, they will usually be in the weaker position when contracting with businesses for use of their personal information. Businesses may have more money and legal resources to draw upon when entering negotiations and agreeing to the final terms of a license. They also may have well-established terms and conditions that consumers must either accept or walk away from altogether.

UCITA gives individuals the right to uses of their information that may be difficult for them to obtain on their own. For example, section 307 provides that "[n]either party is entitled to any rights in new versions of, or improvements or modifications to, information made by the other party."[110] Individuals benefit from this provision because it means companies will not have rights to any new information these individuals generate about themselves unless there is a provision in the licensing agreement allowing for it. If an individual changes her address or name, a company that has licensed to use her information in a database for $2.00 would not be able to use this new information unless a new licensing agreement was made. Problems could arise under this provision of UCITA, though, because companies will not want to re-contract every time an individual's information changes. The system would therefore work more productively if licensing agreements actually specified a time period during which information about an individual could be obtained and collected. For example, individuals could specify that a company may only collect and use information they generate between January of 2000 and December of 2005. This is especially necessary when individuals have contracted with a company to allow them to see their online habits. This information would change every day, even every hour, and companies should not have to create a new contract each time new information is generated. As this example shows, UCITA can be a useful tool for consumers because it sets forth legal standards for licensing agreements that they may be unable to negotiate or enforce themselves.

UCITA not only sets out some basic standards for licensing agreements, but it also provides certain terms that the average consumer may not

---

they currently enter into and often find themselves unhappy with the terms or conditions to which they agree.

110. UNIF. COMPUTER INFO. TRANSACTIONS ACT § 307(d) (Draft, July 1999).

realize she should include in her license agreement. One such provision in section 307 provides that "[i]f a license expressly limits use of the information or informational rights, use in any other manner is a breach of contract."[111] This provision gives consumers the ability to declare unlawful any use of their information that they have not agreed to. Additionally, it empowers the consumer to take legal action if a company which she licenses her information to fails to follow the terms of their agreement regarding the sale of information to third parties, transfers to affiliates or any other provisions of a license designed to protect the individual's privacy. As these examples illustrate, UCITA may give consumers the standard legal protections and rights of enforcement that they might not be able to negotiate for themselves. The law therefore lowers the economic transaction costs and legal confusion of a licensing system and thereby helps to make it a workable solution for the average consumer.

3. *UCITA's Ability to Help Licensors Regulate the Performance of Contracts*

UCITA's provision for the electronic control of contract performance[112] is innovative but controversial. Section 605, "Electronic Regulation of Performance," allows software licensors to repossess software by disabling it remotely.[113] This intrusive step has been at the center of the debate over UCITA.[114] However, these same rights may allow individuals to control the behavior of businesses that violate licenses.[115] An individual could include in her agreement with a business a provision stating that if the information is misused by selling it to an unauthorized third party, or if the

---

111. UNIF. COMPUTER INFO. TRANSACTIONS ACT § 307(b) (Draft, July 1999). This provision gives consumers the ability to declare unlawful any use of their information to which they have not agreed.

112. *See id.* § 605.

113. This type of electronic self-help has been used by vendors such as Logisticon, which shut down Revlon Group's systems because Revlon had not paid the balance on its contract for warehouse management software. *See* Jessica Davis, *Licensing Time Bomb* (May 31, 1999) (visited Apr. 15, 2000) <http://archive.infoworld.com/cgi-bin/displayarchive.pl?/99/22/t33-22.32.htm>; *see also* Robben Rahmen, *Electronic Self Help Reposession and You: A Computer Software Vendor's Guide to Staying Out of Jail*, 48 EMORY L.J. 1477, 1482-93 (1999) (defining electronic self-help and discussing the electronic regulation provisions in UCITA).

114. *See generally* Thomas Hoffman & Patrick Thibodeau, *Rights Usurped Under License Plan*, COMPUTER WORLD, July 26, 1999, at 1; Bob Trott, *Group Attacks Planned Software Licensing Law*, INFOWORLD, Jan. 10, 2000, at 3.

115. Section 605(b) of UCITA reads:

> A party entitled to enforce a limitation on use of information which does not depend on a breach of contract by the other party may include a restraint in the information or a copy of it and use that restraint if: (1) a term of the agreement authorizes use of the restraint; (2) the restraint prevents a use that is inconsistent with the agreement or with informational rights that were not granted to the licensee; (3) the restraint prevents use after expiration of the stated duration of the contract or a stated number of uses; or (4) the restraint prevents use after the contract terminates, other than on expiration of a stated duration or number of uses, and the licensor gives reasonable notice to the licensee before further use is prevented.

UNIF. COMPUTER INFO. TRANSACTIONS ACT § 605(b) (Draft, July 1999).

entity continues to use the information after the contract has ended, the individual may restrict a business's access to that information. This scenario might work in the following way:

> User *A* hires an infomediary that uses a standard license to contract with Company *B* for *A*'s information. The agreement contains a term stating that "*A* can and will use a restraining computer program that will disable *B*'s access to *A*'s information in the event that *B* (1) sells the information to a third party or (2) uses the information beyond the stated duration of the contract." User *B* violates provision (1) of this contract. The infomediary would provide User *B* with reasonable notice before barring User *B*'s access to the information.

There are three complications to using section 605 in the way described above. First, there are technical problems preventing infomediaries from disabling information that has already been transferred to a business. Section 605 works well for the regulation of software use because engineers can program software code to stop working if it is misused, but it might be difficult to write such disabling code into pure information. Even if such code could be written into the information transferred to businesses, controlling misuses of information is much harder than controlling software. Unlike software, personal information does not have to remain on a hard drive so that a computer can perform specific tasks. Information can be printed out and kept in hard copy form. Once information is converted to this medium, it can not be remotely disabled and electronic regulation becomes ineffective. By downloading an individual's information off the Internet and storing it on floppy disks a company could skirt the rules of UCITA and use the information in ways that would directly violate the license agreement. This problem could be resolved if it were possible to program electronic agents to alert an individual whenever their information was downloaded from the Internet without permission. However, this system would be very time consuming for the user. A final problem with using electronic agents to monitor licensees' compliance with contracts concerns what happens to the information once the agreement expires. It is unlikely that an infomediary will be able to detect abuses that occur after the expiration of a contract.[116] For these reasons, section 605 does not provide information licensors with a viable means for regulating performance of their licenses.

116. If an individual is able to find out that a company has used her information after the license has ended, UCITA does consider this a breach of contract under section 618(b). But how one catches a company using information after the license has terminated remains problematic.

4. UCITA Could Protect Commercial Entities

UCITA could also protect businesses if resourceful individuals try to use the licensing system to make quick money by providing businesses with false information. While most corporations would most likely include a warranty provision in their contract, smaller companies and Internet Web sites may not have lawyers to help create licenses with these clauses. Small commercial entities therefore will be the ones to benefit the most from section 404 of UCITA which provides an implied warranty in informational content. The provision states that "[u]nless the warranty is disclaimed or modified, a merchant that, in a special relationship of reliance with a licensee, collects, compiles, processes, provides, or transmits informational content, warrants to its licensee that there is no inaccuracy in the informational content caused by the merchant's failure to perform with reasonable care."[117]

Whether this provision applies to licensors supplying personal information to businesses hinges on the definition of "merchant." Section 102(47) defines "merchant" as

> a person that deals in information or informational rights of the kind or that otherwise by the person's occupation holds itself out as having knowledge or skill peculiar to the practices or information involved in the transaction, or a person to which such knowledge or skill may be attributed by the person's employment of an agent or broker or other intermediary that by its occupation holds itself as having such knowledge or skill.[118]

Since an individual's personal information constitutes "information" under UCITA,[119] an individual or her infomediary would be a "merchant." She therefore would be responsible for acting with reasonable care to provide a business to which she licenses information with accurate personal information. This warranty makes it easier for small businesses to participate in licensing agreements and to prosecute fraudulent submissions of information. UCITA therefore helps to give both the consumer and the business contracting for information confidence in the licensing system by making provisions for abuses of information agreements.

C. The Shortcomings of Information Licensing Systems Under UCITA

It is difficult to apply a law designed for software licenses to information licenses. With some manipulation, UCITA provides a framework for understanding issues of liability, contract formation, and warranty. The Act allows individuals to create standard form agreements that infomediaries can use to negotiate deals and enter agreements with vendors. These

117. UNIF. COMPUTER INFO. TRANSACTIONS ACT § 404(a) (Draft, July 1999).
118. *Id.* § 102(47).
119. *See supra* text accompanying notes 98-107.

agreements give individuals the right to control the collection, use, and exchange of their information, and to use electronic agents to negotiate licensing terms. Despite these useful applications of UCITA, there are still some improvements that need to be made in order for this Act to be an effective legal framework for an information licensing system.

An information licensing system that seeks to protect consumers' personal information, while providing commercial entities with useful data, must be premised on a legal right to privacy. UCITA provides a legal basis for contracting this right but not for establishing it. For the United States to make privacy a priority in both the online and offline worlds it must dispose of its ad hoc approach to privacy and develop a law that provides comprehensive protection to all forms of information. This protection can be achieved by following Europe's example and declaring information privacy a basic right.[120] Once privacy has been cemented as a right, the legal structure of UCITA can be used to license that right on the Internet.

Unless this basic right to information privacy is grounded in our country's federal laws, there will not be an across the board adoption of the licensing system amongst the commercial sector of the Internet community. UCITA alone cannot achieve compliance because it does not create incentives to license personal information. Unless it becomes illegal to use an individual's personal information without a license, businesses will only be driven by market incentives to license information from consumers rather than obtain it for free. A licensing system based on market incentives will encourage responsible businesses to enter licensing agreements and follow the terms of the contract, but will have no effect on businesses that are not concerned with customer service or their reputation among consumers. Additionally, under a licensing system governed by UCITA, third parties will not be bound by the original license agreement made between a consumer and a business. Thus, if a business sells a consumer's information to a third party, the third party will not be bound by the terms and conditions of the license. If a right to privacy is established, entities then will have an incentive to enter licensing agreements and follow certain basic privacy principles.

If a basic right to privacy is established in this country, a licensing system for personal information might not be needed at all. If our government were to set forth basic privacy principles that all businesses and individuals were required to follow, consumers might no longer need licenses to protect their privacy. However, while the right to privacy may stop

120. This basic right to privacy is evidenced by the fact that in "most European countries, personal data protection is a constitutional principle and the right to privacy is enshrined in the Europe Convention on Human Rights." *Directive on Personal Data Protection Enters Into Effect* (Oct. 23, 1997) (visited Nov. 1, 1999) <http://europa.eu.int/comm/internal_market/media/dataprot/news/925.htm>.

abuses of information, it will most likely not be able to meet the two most important goals of a privacy system as defined in this paper: consumer control over information and the right to benefit from its disclosure. A licensing system is the best way to achieve these goals since it gives consumers control over their information, allowing them to decide with which businesses to share their data and how much sensitive information to share. Under a licensing system, individuals would also be able to negotiate through a licensing agreement a benefit for the disclosure of their information. The level of control that a licensing system allows and its support of the commodification of information makes it a viable means for obtaining the type of privacy this Comment discusses. The value of this system therefore would not be lost even if a basic right to privacy was established.

If UCITA is to be used as the legal framework for a personal information licensing system it must address certain problems with its application to these agreements. First, it is difficult to apply some of the sections in UCITA to personal information.[121] The result is that personal information licenses will not be governed by a comprehensive law but by selective sections of UCITA. This discrepancy will create a tremendous amount of confusion for licensors, licensees, and lawyers when they attempt to determine which parts of the Act apply to information licenses. When people are licensing something as important and sensitive as their personal information, it is difficult to govern that process with a law designed to regulate a different commercial product.

Second, UCITA does not provide a viable means for regulating businesses' adherence to the terms and conditions of the licensing agreements they enter. As discussed in Part IV.B.3, the use of electronic self-help permitted under section 605 does not empower the licensor of personal information. An individual cannot remotely disable and repossess their information when an abuse has occurred in the same way that a software licensor can with their product. Under UCITA, individuals do not have a viable means for regulating a licensee's use of their information and stopping abuses when they occur. However, this problem may be better resolved through technical solutions rather than legal changes. Infomediaries may be able to embed code in every piece of information a consumer licenses to make it impossible to use the information in ways that are prohibited under the agreement. In resolving the problems that occur with a licensing system under UCITA, it is important to remember that many of

121. See *supra* notes 98-107 and accompanying text for a discussion of the difficulty in fitting personal information under the scope of UCITA; see also *supra* notes 112-116 and accompanying text for a discussion of the ineffectiveness of electronic agents under section 605 for monitoring the performance of information licensees and the failure of the remedies section of UCITA to meet the needs of the information licensor.

the issues that arise are better resolved through technical rather than legal means.[122]

Third, if UCITA is adopted by all 50 states,[123] it will "make the law [regarding computer information transactions] uniform among the various jurisdictions."[124] However, UCITA fails to recognize the fact that there are no national boundaries on the Internet.[125] Laws governing cyberspace should be international in scope rather than domestic. Consumers who rely on UCITA's provisions may find themselves without a cause of action when dealing with a foreign business. Additionally, large American businesses will be quick to recognize that foreign businesses can obtain information for free, whereas domestic businesses have to contract for the right to that information. Businesses will easily be able to skirt UCITA by running their Web sites from foreign locales. This practice cannot be prevented simply through amendments to UCITA, but will need to be resolved through international discussions about jurisdiction and enforcement issues on the Internet.[126]

Fourth, while UCITA provides for the enforcement of personal information contracts via electronic agents and warranty provisions, it also needs to give individuals and businesses some type of remedy for abuses. Remedy structures are important in personal information licensing systems

---

122. For an in-depth discussion of how technology can resolve different legal and policy issues that arise on the Internet, see Tom W. Bell, *Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557, 619 (1998) (discussing the technology of digital rights management systems as part of the solution to copyrighted material on the Internet, and noting that automated rights management can be used to replace fair use with "fared use" which would require consumers to pay for the right to access and re-use information); *see also Developments in the Law—The Law of Cyberspace*, 112 HARV. L. REV. 1634, 1635 (1999) (suggesting that altering the architectural code of the Internet may be a better answer to problems in cyberspace than the law because technological solutions are more capable of responding to the fast pace, changing environment of the Internet); Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 555 (suggesting that "rules for information flows imposed by technology and communication networks" can be used to help solve policy problems on the Internet).

123. Although the attorney generals from twenty-six of the fifty states have denounced the proposed law, *see* Bray, *supra* note 95, it has already been adopted in Virginia, *see* Craig Timberg, *Gilmore Signs Bill on Software*, WASH. POST, Mar. 15, 2000, at B1, and will most likely be adopted by several other states by the time this Comment is published. For an update on UCITA's progress in the states, see *What's Happening to UCITA in the States* (visited July 16, 2000) <http://www.UCITAonline.com/wbathap.html>.

124. UNIF. COMPUTER INFO. TRANSACTIONS ACT § 106(1)(D) (Draft, July 1999).

125. *See* David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1378-79 (1996) (suggesting that laws based on terrestrial borders do not work in cyberspace; laws should be designed to treat cyberspace as a "place" separate from the "real world").

126. On June 8-9, 1999, the FTC hosted a conference entitled *US Perspectives on Consumer Protection in the Global Electronic Marketplace* to address these issues. Representatives from the United Kingdom, Norway, Italy, Japan, Canada, Australia, and the United States came together to debate and discuss issues of jurisdiction and choice of law for consumers in the electronic marketplace. The materials from these talks can be found at <http://www.ftc.gov/bcp/icpw/990609global.pdf> (visited July 16, 2000).

for two reasons: (1) they compensate the injured party, and (2) they give each party an incentive to follow the terms of the license. Unfortunately, the remedy structure of UCITA fails to achieve these goals.

Breach of contract under UCITA does not allow for punitive damages but only entitles a licensor to damages that cover the amount the licensor lost due to the breach.[127] Under section 808, which specifies a licensor's damages, an individual who licenses her information to a business will not be able to receive very much in damages for a breach.[128] A contract for an individual's information would most likely range from negligible values to several thousand dollars.[129] The cost of attorneys' fees to sue for breach of contract would therefore often far exceed the amount recoverable. It would be economically inefficient for a party to sue for compensation of their injury.

If the damages award could take into account factors such as harm to the individual through the misuse of their information and loss of future contracts as a result of the dissemination of their information in the marketplace, then damages could be pushed higher. However, section 808(1) of UCITA limits this possibility. It specifies that damages can be "measured in any combination of the following ways but [are] not to exceed the contract fee and the market value of other consideration required under the contract for the performance that was the subject of the breach."[130] UCITA therefore fails to provide information licensors with an adequate damage structure for breach of contract.

Even more importantly, the Act fails to give individuals an effective remedy for breach of contract; UCITA does not include a provision for injunctive relief. Licensors of personal information are likely to care more about obtaining injunctive relief against a business that is misusing their personal information than receiving monetary damages for breach of contract.[131]

The remedy structure of UCITA not only fails to compensate individuals for their injury but it also fails to provide parties with incentives not to breach contracts. The low damage awards and lack of injunctive relief make UCITA ineffective as a means for deterring individuals from ignoring the terms of their contracts. Since the consequences of breach are not high, it may actually be more profitable for businesses to sell

127. *See* UNIF. COMPUTER INFO. TRANSACTIONS ACT § 808(b)(1)(A)-(D) (Draft, July 1999).

128. *See id.*

129. These figures are just an estimate of how much money consumers could receive for information. It is more likely that companies will give customers items such as frequent flier miles, discounts on products, customized service or gifts such as computers, than money. *See supra* note 30.

130. UNIF. COMPUTER INFO. TRANSACTIONS ACT § 808(b)(1) (Draft, July 1999).

131. Under section 802, the aggrieved party may cancel the contract and thereby cut off the licensee's ability to use the information. Section 803(a)(1) also states that parties may modify their contract to account for remedies not included in UCITA.

consumers' personal information in breach of a license agreement, and risk paying a minimal damage award, than to adhere to the terms of the agreement. Similarly, an individual may find it more profitable to provide fraudulent information than to comply with UCITA's implied warranty clause.[132]

While UCITA does not provide an incentive to stop bad actors, the market might actually fill this role for commercial entities. If a business decides to breach its contract by selling a consumer's information, it will not only have to deal with bad press coverage but it may be unable to enter licensing agreements with other customers after its actions are disclosed. The reality of licensing agreements under UCITA, therefore, is that there are few legal incentives for either party to follow the terms of its agreement.

In conclusion, UCITA lays the groundwork for online contracting by applying traditional contracting principles such as offer, acceptance, and performance to the Internet. However, it does not constitute a U.C.C. for the Internet. A comprehensive set of rules for cyberspace will take time to develop and will require an understanding of all types of Internet contracts, now existing and still to be conceived, rather than just online software licenses. As the Internet and the laws governing it develop, the NCCUSL may resolve some of the problems with UCITA I have discussed. Among the issues that the NCCUSL will need to address are: the limited domestic scope of UCITA; the inability of licensors to track and prevent violations of the license; the lack of a sufficient remedy structure for personal information licenses; and the ad hoc protection given to information licenses. Once a basic legal right to privacy is established in this country and the current problems with UCITA are addressed, the Act will provide a sufficient legal framework for a personal information licensing system.

V

IDEALLY AN INFORMATION LICENSING SYSTEM WILL BE ABLE TO ACHIEVE THE GOALS OF INTERNET PRIVACY

Currently the Internet only has information dating back five or six years, but as our everyday transactions become increasingly connected to this medium, there will be more at stake in terms of the use and dissemination of our online personal information. One infomediary, Lumeria, predicts that eventually every electronic device will be connected to the Internet so "a person can be monitored as they drive their car, use their stereo or TV, or open the refrigerator. In short, their privacy can

132. *See supra* Part IV.B.4.

be . . . obliterated."[133] A privacy solution for today's electronic marketplace should be designed to meet the challenges this vision of the future presents.

An online licensing system governed by UCITA can meet the challenges of this future. The system has the potential to successfully meet all six of the goals set out in this Comment once it is implemented. First, licensing personal information gives the individual choice. Consumers can negotiate the terms of a contract or refuse altogether to enter into agreements that do not limit the number of third parties who view their information or control how their data is used. Second, a licensing system provides consumers with notification of how their personal information is being used via the terms of their licensing agreement. If an infomediary enters into the contract for the consumer, it should alert the individual to any aspects of the contract that exceed the form terms that the person agreed to when they registered with the infomediary. Third, the licensing system could provide the individual with a means to verify that a business's privacy policies are being followed. This verification could be achieved by having privacy seal providers work with infomediaries to monitor businesses' adherence to licenses.[134] Fourth, the licensing system allows individuals to receive compensation for the use of their personal information. Fifth, infomediaries could make this system easy to use by handling the contract initiation, negotiation, and approval.[135] Sixth, a licensing system could provide for enforcement of contract terms if advances were made in the application of electronic self-regulation to personal information.[136] Additionally, UCITA provides consumers with damages as redress for breach of a contract.[137] An information licensing system therefore meets the goals of an effective privacy solution. However, the social implications of this system must be carefully considered before adopting it as the answer to Internet privacy.

A. Redlining in Cyberspace

If businesses can find out everything we do, what effect will this have on society? One of the benefits of the Internet is the freedom it gives individuals to escape the visual categorizations of the real world. In cyberspace, individuals can choose to either hide or reveal race, gender, income level, or sexual preferences. As commercial entities begin to farm the Internet for information, and individuals become comfortable enough with the medium to share more intimate details of their lives, the discriminatory practices of the real world may infiltrate the Internet.

---

133. *What is Privacy?* (visited Apr. 5, 2000) <http://www.superprofile.com/paper1/privacy1.html>.

134. *See* discussion *supra* Part III.C.

135. *See* discussion *supra* Part IV.B.1.

136. *See* discussion *supra* Part IV.B.3.

137. *See* discussion *supra* Part IV.C.2.

Using zip codes and telephone numbers as signals, businesses can determine where consumers live. Businesses can target specific customers and market their products to people in areas that they predict would be interested in what they are selling. For example, in the Internet context, a business selling airline tickets would want to know that some of the users on "surf.com" live in Hawaii. They could then offer special flights to surf competitions on the mainland to the site's Hawaiian users. However, there is a fine line between this type of targeted marketing and redlining. Redlining occurs where companies choose not to sell their products to a certain group of customers based on factors such as income level or race. Users' zip codes or the information they volunteer also could be used to discriminate amongst customers. For example, businesses could recognize zip codes from low-income areas and choose not to advertise to these groups or could make decisions about an individual's insurance policy based on information they collect about them on the Internet.[138] These types of discriminatory uses of individuals' personal information would limit autonomy.[139]

Businesses create a profile of us based on the information we provide on the Internet. Using this picture they can discriminate against us just as easily in the virtual world as they can in the real world. A licensing system that gives consumers control over who can collect and use sensitive information about their race, medical history, or income level may help to limit this problem. But ultimately this problem cannot be resolved through a licensing system alone. The solution depends on the government, businesses, and online communities adopting good information practices and expressing a commitment to keeping the Internet free of real world discrimination.

B. The Demarcation of the Information Poor

The commodification of personal information highlights another social issue: the struggle between the information rich and the information poor in our modern world. If personal information becomes a commodity that can be licensed, the licensors in this system will not be the information rich who already have computers, cable connections, email accounts, and money. These individuals will not need to exchange their personal information in return for becoming part of the Internet community. Instead, the users of this system will be the individuals who are too poor to afford

138. *See generally* John Markoff, *Converting E-Mail from Spam to Steak*, N.Y. TIMES, Sept. 22, 1999, at G64 (diseussing the use of email for direct marketing campaigns). The Electronic Freedom Foundation eriticizes such campaigns, noting that "[t]here is a fine line between targeting and redlining . . . what if an insurance company or an H.M.O. knows that you're reading about cancer or alzheimer's disease on line? They may decide not to issue you an insurance policy or provide health care." *Id.*

139. *See supra* text aecompanying notes 45-46.

computers and cannot pay for a monthly Internet connection fee; they will sell their personal information to marketers to receive these benefits. Privacy will become a luxury only the rich can afford. This possibility begs the question of whether our personal information should be a commodity for sale.

Even if personal information does become a commodity, not all such information will be equally valued. The majority of businesses who want information about individuals want it so that they can sell that person something. In a world where personal information is sold to the highest bidder, the seller will most likely be poor. Marketers may be less able to sell products to individuals who do not even have the money to pay for their connection to the Internet. A licensing system may not meet the needs of businesses if it leads to the collection of information from the "wrong" group of consumers. We can take comfort in the fact that the world is not as polarized as I have just painted it; there is still the middle class who will license their information when the benefit is useful or lucrative enough. It is important to recognize though that a licensing system is most attractive to the groups that are least attractive to marketers.

C. A Comprehensive Solution to Online and Offline Privacy.

An effective licensing system must apply to information collected in both the online and offline worlds. The licensing system proposed in this Comment only provides individuals with a workable solution for controlling the information they generate or provide over the Internet. Since infomediaries and the legal framework of UCITA do not govern "real world" transactions, individuals are not able to control the collection and use of their ATM transactions, credit card purchases, telephone number, address, employer's name, social security number or other "real world" sensitive information. A viable privacy solution for the modern electronic marketplace must be able to protect all of an individual's information in both the online and offline worlds.

In the international marketplace of our modern world, a comprehensive solution to privacy will not come from Internet-centric systems such as anonymizers, privacy seal programs, or even licensing systems. The answer lies in using these systems to support a federally recognized right to privacy and international standards for protecting it. Until this occurs, there will not be a comprehensive and effective solution to the loss of virtual privacy.