

# The Consumer Privacy Debate by David Rair and Rene Chinen

## WHAT IS THE PRIVACY DEBATE ABOUT?

During the last several years, much has been written about consumer privacy.<sup>1</sup> Changes in how personal information is gathered and used have focused attention on the potential for abuse. The debate has grown as businesses have attempted to use consumer information to sell consumer lists or personal spending information to retailers and other users.<sup>2</sup> In addition, with the ever-increasing use of the internet for a wide variety of purposes, such as applying for loans, purchasing goods, doing on-line banking, and expressing personal opinions, recipients of transactional information and other personal information can use information provided for purposes unrelated to the original transaction or sell the information to third parties.<sup>3</sup> Although the collection and use of information through the internet has intensified the debate, the use of consumer information has been an issue for many years.

Because of growing concern over potential abuse of consumer information, government agencies, private industry and consumer privacy groups have been debating the need for government regulation in this area. The primary concerns are that consumers may not be aware of the consequences of providing personal information and that they may not have any remedies if information is inaccurate, misused or sold without their permission. The current view is that private industry should self-regulate its use of consumer information.<sup>4</sup> This view, however, has recently come under criticism, and consumer groups, government agencies and Congress have questioned the effectiveness of self-regulatory efforts.<sup>5</sup>

## TRADITIONAL SOURCES OF PRIVACY LAW UNDER STATE LAW.

Under state law, the regulation of privacy exists at three levels. First, in addition to limits on a state's right to search and seize private information, state constitutions may limit a businesses' ability to disclose personal or financial information to third parties. For example, under the Hawaii Constitution, a person has the right to be secure against "unreasonable invasions of privacy" in addition to the right to be secure against unreasonable searches and seizures.<sup>6</sup> In addition, the Hawaii Supreme Court has held that the right to be secure against unreasonable invasions of privacy under the Hawaii Constitution extends to actions taken by commercial entities.<sup>7</sup> As to bank records, however, the Hawaii Supreme Court has held that there is no reasonable expectation of privacy in such records.<sup>8</sup>

Secondly, many states have specific statutes which regulate the disclosures of financial information.<sup>9</sup> For example, at least one state has enacted a statute which prohibits any corporation from disclosing confidential information.<sup>10</sup> Likewise, Hawaii has enacted statutes which regulate the disclosure of certain financial information. For example, the Hawaii Penal Code prohibits disclosure of the names of credit cardholders without their prior written consent,<sup>11</sup> and the Hawaii insurance code prohibits creditors from using or disclosing insurance policy information for purposes of soliciting insurance.<sup>12</sup>

The third source of privacy rights is a state's common law. The common law theories of defamation, invasion of privacy and implied contract provide



some protection against disclosure of private information, but the protection is limited.

Since the common law theory of defamation protects persons only against the publication of false information about them, it is of limited protection against the disclosure of confidential information.<sup>13</sup> In addition, defamation law contains a number of qualified privileges which protect a person in a business relationship with another from liability when disclosing false information.<sup>14</sup>

The common law theory of invasion of privacy, or the "right to be let alone,"<sup>15</sup> generally protects individuals from the: (1) unreasonable intrusion into a person's seclusion, solitude or private affairs; (2) public dissemination of embarrassing private acts; (3) publicity which places a person in a false public light; and (4) appropriation of a person's name, image or likeness.<sup>16</sup> Although applicable to the acquisition and use of customer information by businesses, the theory does have its weaknesses in the context of privacy issues. For example, the second, third and fourth bases normally do not apply. Consequently, consumers are left with the first basis, which would only apply if a business collects personal information in an unreasonable manner or by an unreasonable means.

The common law theory of implied contract also has been used in the privacy context. First the English courts,<sup>17</sup> and, later, several American courts<sup>18</sup> adopted the theory that a bank has an implied agreement with its customers that the bank will keep the customers' financial affairs confidential except under certain circumstances when disclosure is required or permitted. However, the American courts remain split on whether a confidential relationship will be implied between a bank and its deposit and/or loan custom-

ers. Some courts have found that no such relationship exists, while other courts have held that a confidential relationship may arise when the customer places trust in the bank or in other special circumstances.<sup>19</sup> Although the theory has been principally applied in situations involving banks and their customers and there is no specific case law in Hawaii, there is nothing to prevent the extension of the theory in appropriate circumstances to other financial institutions and to commercial firms in cases where consumers provide confidential information and do not expect that the information will be released to third parties.

Due to the difficulties that can be encountered in using the traditional sources of state privacy law described above, consumers and regulatory agencies are also relying on the use of federal and state unfair and deceptive trade practices' statutes as a means of regulating the commercial use of consumer information collected, used and distributed.<sup>20</sup> Under these statutes, government agencies and private plaintiffs typically allege that a person has committed an unfair and deceptive trade practice by misrepresenting how confidential information provided to the person will be used. As discussed below in more detail, the Federal Trade Commission (the "FTC") recently brought its first enforcement action against a website operator under the unfair and deceptive trade practice provisions of Section 5(a) of the Federal Trade Commission Act.

## **FEDERAL INTERVENTION ON THE BANKING INDUSTRY.**

For many years, there has been an extensive set of federal laws that relate to how financial institutions can use their customers' information. These laws have for the most part been sufficiently flexible to



cope with changes in technology during the past three decades, and continue to apply to customer information that is provided, or gathered, by traditional means or in the on-line environment. For example, the sharing of information obtained from consumer reports obtained in response to consumer credit applications is regulated by the Fair Credit Reporting Act.<sup>21</sup> In addition, federal bank regulators have traditionally regulated how and when financial institutions may use or release confidential information.<sup>22</sup> However, despite the existing statutory and regulatory constraints on the use of consumer information by financial institutions, the information practices of those institutions have received much of the attention created by the privacy debate.

In response, the American Bankers' Association (the "ABA") prepared a white paper in June, 1998, entitled *Financial Privacy in America A Review of Consumer Financial Services Issues*.<sup>23</sup> In the white paper, the ABA summarized the major federal statutes that relate to the use of consumers' financial information, and provided a perspective on how the use of personal information by a bank can benefit the customer. Of course, as an advocate for the banking industry, the ABA has been involved in an effort to discourage additional federal legislation in the "privacy" area, arguing that financial institutions are already very heavily regulated and have historically done more to protect customer confidentiality than any other industry.<sup>24</sup> In order to promote industry self-regulation, in September, 1997, the ABA joined with other banking trade associations<sup>25</sup> to develop a common set of privacy principles. Each association has encouraged its members to adopt privacy principles and procedures based on these industry guidelines.<sup>26</sup>

Similar to the approach taken by the banking industry, the Clinton Administration and the federal banking regulatory agencies have consistently expressed the view that they favor industry self-regulation as an alternative to new federal legislation.<sup>27</sup>

Nevertheless, in 1998, with the privacy issue in the national spotlight, the federal banking regulatory agencies began to take a more active role. On August 17, 1998, the Federal Deposit Insurance Corporation ("FDIC") published Financial Institution Letter ("FIL") 86-98, entitled *"Electronic Commerce and Consumer Privacy."* The attachment to this FIL, *"Online Privacy of Consumer Personal Information,"* encouraged financial institutions to:

*"...maintain an awareness of emerging consumer online privacy concerns, and to take voluntary, specific actions to address them. In particular, financial institutions should provide meaningful disclosures of privacy policies and information practices, and effectively enforce these policies and practices."<sup>28</sup>*

In FIL 86-98, the FDIC specifically points out that self-regulation can only be effective when it is accompanied by "employee education, adequate internal controls, and meaningful enforcement and redress."<sup>29</sup> Thus, although FIL 86-98 is stated to be a "guideline," as a practical matter, banks supervised by the FDIC will be expected to comply with the FDIC's suggestions.

Similar guidelines have already been issued by other bank regulatory agencies. In November, 1998, the Office of Thrift Supervision ("OTS") issued a policy statement which contains information similar to the FDIC's guidelines. In its statement, the OTS specifically points out that the terms of the policy statement will be considered by examiners when



evaluating the institution's internal controls.<sup>30</sup> This is clearly a step beyond a "recommendation" and effectively signals the beginning of regulatory oversight on financial institutions' information practices.

### **OTHER REGULATORY INITIATIVES.**

In addition to the banking regulators, other federal agencies, such as the FTC and the Department of Commerce (the "DOC"), have been actively involved in the privacy debate. Although the FTC and DOC have publicly advocated self-regulation, both agencies have increasingly warned that industry's self-regulatory efforts to date have fallen short, and the FTC has been increasing its enforcement activities in this area.<sup>31</sup>

The FTC held its first public workshop on privacy in April 1995, and held a series of hearings in October and November 1995 on consumer protection and privacy issues relating to technological innovations in the marketplace. In June, 1996, the FTC held an additional workshop and examined many other topics, including commercial website practices with respect to the collection, use and transfer of consumer information. Based on the June 1996 workshop, the FTC published a staff report entitled *Consumer Privacy on the Global Information Infrastructure*.<sup>32</sup> Also, in June, 1998, the DOC issued a request for comment on its staff "discussion paper" entitled Elements of Effective Self Regulation for Protection of Privacy in which the DOC outlined its principles of fair information practices.<sup>33</sup>

In June, 1998, the FTC issued Privacy Online: A Report to Congress in which the FTC reported that, of the 1,400 web sites surveyed, roughly 85 percent collected personal information about consumers who visited those sites.<sup>34</sup> In addition, the FTC found that,

while 97 percent of the 125 financial sites surveyed collected personal information, only 16 percent disclosed their practices on collecting information.<sup>35</sup> The FTC concluded that "industry's efforts to encourage voluntary adoption of the most basic fair information practices have fallen short of what is needed to protect consumers."<sup>36</sup> Finally, on July 21, 1998, the FTC presented an online consumer privacy legislative model in testimony before the House Subcommittee on Telecommunications, Trade and Consumer Protection. Under its legislative model, the FTC would require all commercial websites to comply with certain information practices including notice, choice, security and access requirements. In addition, the FTC reiterated its position that private industry would have until the end of the year to implement broad-based and effective self-regulatory programs or the FTC would recommend specific legislation to Congress.<sup>37</sup>

As the FTC has become increasingly more critical of industry's efforts at self-regulation, the FTC has started to bring enforcement actions against website operators. For example, in August 1998, the FTC entered into a settlement agreement and consent order with GeoCities, a popular website. The GeoCities website is a "virtual community" consisting of member's personal home pages organized by theme areas called neighborhoods. Individuals who wish to become members must complete an application consisting of mandatory and optional information. Applicants could also choose to request and receive special offers and merchandise from selected advertisers and companies.

In the complaint, the FTC stated that GeoCities misrepresented the purposes for which it collected personal identifying information. Specifically, the



FTC alleged that GeoCities engaged in deceptive practices in the way it collected information by falsely stating that identifying information would not be provided to third parties, and that information would be used only to provide specific advertising offers consumers request when, in fact, the information was provided to third parties for other uses. In addition, the FTC alleged that GeoCities failed to accurately disclose its information collecting practices by stating that it collected information when, in fact, third parties were collecting the information.<sup>38</sup>

Rather than fighting the FTC, GeoCities entered into a settlement agreement with the FTC which among other things: (1) prohibits GeoCities from misrepresenting its collection and use of personal identifying information including what information will be disclosed to third parties; (2) prohibits GeoCities from misrepresenting the identity of persons collecting such information on its website; (3) prohibits GeoCities from collecting such information from a child if GeoCities learns the child does not have parental permission to provide the information; (4) requires GeoCities to clearly disclose its information practices; (5) sets forth parental choice and control principles; (6) sets forth requirements with respect to previously collected information; and (7) establishes certain recordkeeping requirements.<sup>39</sup>

## CONCLUSION.

With all of the public concerns regarding privacy generally and with the increase in regulatory and enforcement activity, businesses of all types and sizes will want to be aware of the privacy issue and to consider taking active measures to ensure that they do not become targets of government agency enforcement actions or private plaintiff litigation.

[www.chunrair.com](http://www.chunrair.com)  
808.528.4200

## About the Authors

David Rair is a partner at Oshima Chun Fong & Chung. Rene Chinen is in the legal department at First Hawaiian Bank.

You can contact David Rair at 808.528.4200, or email him at [drarir@chunrair.com](mailto:drarir@chunrair.com)

© 2006, all rights reserved

## ENDNOTES

<sup>1</sup> See, e.g., Robert O'Harrow Jr., "For Sale on the Web=Your Financial Secrets," *Wash. Post*, June, 1998, at A1; Leslie Miller, "No Solitude in Cyberspace," *USA Today*, June 9, 1997, at ID; Anne Gearan, "Recipient of Junk Mail Sues Magazine that Sold his Name," *Honolulu Advertiser*, Feb. 7, 1996; and "Netscape Finds Hawaii in Browser," *Star-Bulletin*, June 13, 1997.

<sup>2</sup> See, e.g., Bruce Horowitz, "AmEx to Sell Information About Consumers," *USA Today*, May 13, 1998; Tami Liliby, "First Union=Data Warehouse Revenue \$100 Million a Year," *Am. Banker*, June 12, 1998; Lisa Fickenscher, "American Express Seeks to Mine its Data on Cardholder Spending Platforms," *Am. Banker*, Mar. 24, 1997; See also "Data Warehouse Market Booming," *Am. Banker*, Sept. 9, 1998.

<sup>3</sup> *Id.*, See also, Joanna Smith Bers, "Secrets for Sale," *Future Banker*, August 1997, at 38; and "Surfer Beware; Personal Privacy and the Internet" (Elec. Privacy Info. Ctr., Wash. D.C.), June 1997 available in <http://www.epic.org>.

<sup>4</sup> See, Bill McConnell, "Privacy Danger Seen as Mergers Multiply Chances to Cross-Sell," *Am. Banker*, May 11, 1998; See also "ABA Explains Banks' Consumer Privacy Position, Urges Congress to Call on Industry to Self-Regulate," *News (Am. Bankers Assoc., Wash. D.C.)*, Sept. 18, 1997; and Alex D. McElroy, "Williams Urges Banks to Take Lead in Protecting Consumers' Private Information," *Banking Reg. (Bureau of Nat'l Aff., Wash. D.C.)* May 18, 1998, at 797.

<sup>5</sup> See, Bill McConnell, "Banker Under New Rescue to Protect Privacy—or Else," *Am. Banker*, Aug. 11, 1998, see also "Bank Associations Attack Feds' Claims that Banks Lack Privacy Rules," *ABA Banking J.*, Aug. 1998, at 8; and "Acting Comptroller Julie L. Williams Urges Industry Leadership on Consumer Privacy," *News Release (OCC, Wash. D.C.)*, May 8, 1998, NR 98-50.

<sup>6</sup> Hawaii Const. Art. I, § 6.

<sup>7</sup> *Fergerstrom v. Hawaiian Ocean View Estates*, 50 Haw. 374 (1968).



<sup>8</sup> *State v. Klatenhoff*, 71 Haw. 598, 606 (1990) (adopting rule in *United States v. Miller*, 425 U.S. 435 (1976)).

<sup>9</sup> See, e.g., Cal. Gov't Code § 7460-7493 (Deering Supp. 1990); Me. Rev. Stat. Ann. Title 9-3, §§ 162-164 (West Supp. 1989); Utah Code Ann. § 78-27-45 (Michie Supp. 1989).

<sup>10</sup> Neb. Rev. Stat. § 8-1401 (1987).

<sup>11</sup> Haw. Rev. Stat. Title 27, § 708-8105 (Michie 1994).

<sup>12</sup> Haw. Rev. Stat. Title 24, § 431: 13-104(a)(4) (Michie 1998).

<sup>13</sup> See, e.g., W. Page Keaton, *Prosser and Keaton on the Law of Torts*, § 117 at 849 (5<sup>th</sup> ed. 1984); Restatement (Second) of Torts § 577 (1981).

<sup>14</sup> See, *Prosser and Keaton on the Law of Torts*, supra note 12, § 115 at 833; Restatement (Second) of Torts, § 600 (1981).

<sup>15</sup> Warren & Brandeis, "The Right to Privacy", 4 Harv. L. Rev. 193 (1890).

<sup>16</sup> See, *Prosser and Keaton on the Law of Torts*, supra note 12, § 117 at 851, 854, 856, 863.

<sup>17</sup> *Tournier v. National Provincial & Union Bank of England*, 1KB 461 (1923).

<sup>18</sup> *Peterson v. Idaho First National Bank*, 367 P.2d 284 (Idaho 1961); *Division of Pari-Mutuel Wagering v. Winfield*, 443 So. 2d 455 (Fla. Dist. Ct. App. 1984); *Suburban Trust Co. v. Waller*, 408 A.2d 748 (Md. 1979).

<sup>19</sup> See, *Reid v. Key Bank of Southern Maine, Inc.*, 821 F.2d 9 (1<sup>st</sup> Cir. 1987).

<sup>20</sup> See, e.g., *Dwyer v. American Express Co.*, 652 N.E. 2d 1351 (Ill. App. Ct 1995); *In re GeoCities*, Complaint, F.T.C. (1998).

<sup>21</sup> 15 U.S.C. § 1681, et seq.

<sup>22</sup> See, e.g., OCC Interpretive Letter No. 316 (December 4, 1984); 12 C.F.R. Part 545 (1989).

<sup>23</sup> The white paper is available on the ABA's web site: <http://www.aba.com>.

<sup>24</sup> ABA white paper, page 1.

<sup>25</sup> Other associations include The Bankers Roundtable and its division the Banking Industry Technology Secretariat, the Consumer Bankers Association, and the Independent Bankers Association of America.

<sup>26</sup> See, e.g., "U.S. Banking Industry Privacy Principles" available on the ABA web site.

<sup>27</sup> See, supra note 4.; OCC News Release 98-50; May 8, 1998.

<sup>28</sup> See FIL-86-98.

<sup>29</sup> *Id.*

<sup>30</sup> OTS "Policy Statement on Privacy and Accuracy of Personal Customer Information," November 3, 1998.

<sup>31</sup> This may also be due in part to the U.S. government's interest in the impending European Union Directive on Data Protection which requires countries doing business within the European Union to have adequate privacy controls. Failure to do so could result in a prohibition on data transfers between European Union member countries and the offending country.

<sup>32</sup> *Consumer Privacy on the Global Information Infrastructure*, F.T.C. Staff Rep. (Dec. 1996).

<sup>33</sup> 63 Fed. Reg. 30729 (June 5, 1998).

<sup>34</sup> *Privacy Online: A Report to Congress*, F.T.C. Staff Rep. (June, 1998).

<sup>35</sup> FTC Press Release June 4, 1998, citing "Privacy Online: A Report to Congress." This report also deals extensively with the issues on collecting information from children.

<sup>36</sup> *Consumer Privacy on the World Wide Web Before the Subcommittee On Telecommunications, Trade, and Consumer Protection of the House Committee On Commerce*, 105<sup>th</sup> Cong. (July 21, 1998) (prepared statement of the F.T.C.).

<sup>37</sup> *In re GeoCities* Complaint, F.T.C. (1998).

<sup>38</sup> *In re GeoCities Agreement Containing Consent Order*, F.T.C. (File No. 9823015) (1998).

