PRIVACY AND CUSTOMER RELATIONSHIP MANAGEMENT: CAN THEY PEACEFULLY COEXIST?

Christopher K. Sandberg[†]

I. INTRODUCTION 1147
II. CRM 1148
A. *Background* 1148
B. *Why Are Businesses Interested in CRM?* 1148
C. *What do Customers Think?* 1149
III. FAIR DATA PRINCIPLES 1151
A. *Overview* 1151
B. *Application of the Fair Data Principles to CRM* 1153
IV. WHY SHOULD MANAGEMENT CARE ABOUT PRIVACY? 1155
V. OTHER LAWS ON PRIVACY WITH POTENTIAL CRM IMPACT 1158
VI. CURRENT STATUS OF PRIVACY AMONG BUSINESSES 1160
VII. CONCLUSIONS AND RECOMMENDATIONS 1162

I. INTRODUCTION

Customer Relationship Management ("CRM") is one of the hottest topics for businesses entering the age of e-commerce. CRM is often described as the processes and systems that help companies better understand and service their customers. It includes the gathering, manipulation, storage, and analysis of many forms of data about a company's customers. CRM advocates maintain that it can identify the most profitable of a company's customers, lead to a richer product set being offered to customers, improve sales opportunities for the business, and improve customer acquisition and retention.

Since a key component of CRM is the acquisition and storage

[†] Mr. Sandberg is a partner in the Minneapolis law firm of Lockridge Grindal Nauen PLLP, where he practices in the areas of technology, on-line, and telecommunications law. He is also an Adjunct University Associate Professor at St. Mary's University of Minnesota Graduate Center in Minneapolis.

of many data elements about a company's customers, the issue arises of how to balance the company's desire to collect and use personally identifying information with customers' desires to protect their privacy and control others' use of information about them.

This article will examine the legal and policy implications of CRM, and consider issues that arise from the law as it is today and as it is emerging in the United States and the European Union.

II. CRM

A. *Background*

CRM software can be generally described as processes and systems that help companies better understand and service their customers. CRM software began as contact management programs designed to generate more sales leads. While that function remains important to business users, CRM software vendors have added more intelligence to their programs to focus on customer loyalty and retention and "lifetime" customer value.[1] Companies using CRM see value in launching automated marketing programs that target "the right customer . . . at the right time,"[2] or maximizing relations with customers while helping sales, raising productivity, and improving customer morale.[3] Vendors claim that CRM integrates people, process, and technology to maximize relationships with all of a business's customers and partners, including traditional customers, "eCustomers," distribution channel members, internal customers, and suppliers.[4]

B. *Why Are Businesses Interested in CRM?*

According to vendors and industry pundits, CRM can create greater customer loyalty, sales, and satisfaction. In markets characterized by numerous providers of a commoditized product

1. John Berry, *Marketing Automation Gives CRM a Lift,* INTERNETWK., Mar. 20, 2001, *available at* http://www.internetweek.com/indepth01/ indepth032001.htm.
2. *Id.*
3. Mike McCleary, Jr., *Airing CRM's Dirty Laundry*, INTERACTIVE WK., Mar. 26, 2001, at 40.
4. Digital Consulting Institute, *CRM Conference and Exposition Program*, June 20-22, 2001, at 2.

or service, customer service is seen as a differentiator between competing providers. The North American market for CRM software has been projected to "jump from $3.9 billion in 2000 to $11.9 billion by 2005, according to the business information company Datamonitor."[5] The Garner Group has projected worldwide CRM sales to rise from $23 billion in 2000 to $76.3 billion in 2005.[6]

However, industry analysts are starting to recognize that poorly performed CRM can actually tarnish a business's relationship with its customers, and bad CRM can cost a company financially.

C. What do Customers Think?

Customers who are dealing with vendors online report that they want personalization of their interactions with those vendors, but do not trust others easily. In particular, buyers' increased exposure to the Internet has raised both their willingness to provide information and their concerns about its use. These factors, coupled with growing customer demands for more accountability, have placed privacy in the spotlight.

In May and June 2000, a Pew Internet Poll found that 54% of 2,117 U.S. resident respondents (1,017 of whom were Internet users) believed that tracking consumers' online habits is a privacy invasion, but the same percentage had provided personal information in order to use a web site.[7] Ninety-four percent of the respondents believed that the government should punish Internet firms and executives for violating online privacy.[8]

A Cyber Dialogue Survey, also taken in 2000 by the same online market research/database company, found that 38% of 500 online adults who were polled saw a benefit in interacting with a vendor through a personalized Web site with targeted marketing messages, as compared with non-targeted "spam" marketing messages.[9] Of the 500 respondents, 88% said they would give their

---

5. Jim Battey, E-*Business Barometer*, INFOWORLD, Mar. 26, 2001, at 17, *available at* 2001 WL 8083377.

6. *Id.*

7. Susannah Fox, *Pew Internet & American Life Project, Trust and Privacy Online: Why Americans Want to Rewrite the Rules,* Aug. 20, 2000, at 2, *available at* http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf.

8. *Id.* at 3.

9. Kevin Mabey, *Privacy vs. Personalization: Where Do We as Marketers Draw the Line Between Anonymity and One-To-One Communication?*, CYBERDIALOGUE.COM 5 (2000), *available at* http://www.cyberdialogue.com/pdfs/wp/wp-cd-2000-privacy.pdf.

name to a vendor, 90% would give their level of education, age, and hobbies, 59% would give their household income, but only 41% would give their salary, and only 13% would give their credit card number.[10] The respondents in that survey generally agreed they would not accept distribution of their personal information without permission or compensation.[11]

Forrester Research (Forrester) reported similar results in a survey in September 2001, in which "60% of online consumers said they seriously worry about what will happen to the personal information they divulge online."[12] Forrester concluded that the problem this raises for online retailers is that these fears will hold back as much as $15 billion in e-commerce revenue during 2001.[13] While users who have been online consumers longer have lower levels of concern, even after four years of online purchasing over 50% report they remain concerned about privacy.[14] Income, gender, and age have little effect on the degree to which concern is expressed. The leading response to the question of "When do you give out information online?" was "To purchase products or services," followed immediately by "When a site guarantees it won't sell my data."[15] Sixty percent of the respondents said that government should regulate how companies can use customer information.[16]

"[A] February 2001 survey of more than 16,000 online consumers by the research firm cPulse found about half [of the respondents] reported discomfort with the [current] state of online privacy," and almost 60% identifying themselves as "'extremely likely' to return to those commercial Web sites [which permit them to] opt-out of receiving e-mail solicitations."[17]

---

10. *Id.* at 4.
11. *Id.* at 5.
12. *See* Christopher M. Kelley et al., *Privacy Concerns Cost eCommerce $15 Billion*, FORRESTER RESEARCH, Sept. 18, 2001, *available at* http://www.forrester.com/ER/Research/DataSnapshot/Excerpt/0,1317,13484,FF.html. Further survey details were presented in a slideshow for oral presentation entitled "Surviving the Privacy Revolution." *See* Jay Stanley et al., *Surviving the Privacy Revolution*, FORRESTER.COM, Feb. 2001, *at* http://www.forrester.com/ER/Baseline/ QuickView/0,1338,10706,00.html.
13. *Id.*
14. *Id.*
15. *Id.*
16. *Id.*
17. Ted Kemp, *Privacy Tools Emerge, CRM Offerings Aim to Help Companies Respect Consumers' Requests*, INTERNETWK., Apr. 23, 2001, at 15, *available at* http://www.internetweek.com/ebizapps01/ebiz042301.htm.

Consumers are also getting tools to aid in their privacy quest. A company called iPrivacy is developing a private e-commerce service that will let individual consumers shop, buy, and have goods delivered without revealing personal information to any of the ISP's, third parties, or even merchants on the Internet.[18] The software generates a fictitious e-mail address, a one-time credit card number, and an encoded postal address; all these data elements are used only once, for a single e-commerce transaction, so there are no data which the merchant can track, record, use or resell.[19] The software will be distributed through credit card companies.[20]

III. FAIR DATA PRINCIPLES

A. *Overview*

Against this background of businesses' desire to gain more information about their customers and to use that information in more ways, advocates of personal and business privacy point to an emerging set of principles for handling data that contain personal information.

In a 1998 report, *Privacy Online: A Report to Congress*, the Federal Trade Commission ("FTC") summarized widely accepted principles regarding the collection, use and dissemination of personal information.[21] These Fair Information Practice Principles, the FTC said, predate the modern online age and have been recognized and developed by government agencies in the United States, Canada and Europe since 1973.[22] The FTC's report identified the core principles of privacy protection common to the government reports, guidelines and model codes that had emerged as of that time:

(1) *Notice* - data collectors must disclose their

18. James R. Borck, *Enterprise Strategies: Privacy Worries Spell a Recession in Marketing Personalization Data*, INFOWORLD, Feb. 12, 2001.

19. *See generally* iPrivacy *at* http://www.iprivacy.com (last visited Feb. 6, 2002); Margaret Johnson, *CIA-Backed Venture Eyes Anonymity Software,* INFOWORLD, Feb. 12, 2001, at 60, *available at* http://www.infoworld.com/articles/hn/xml/01/02/13/010213hnspy.xml (discussing developments in anonymity software generally).

20. *Id.*

21. FEDERAL TRADE COMM'N STAFF, *PRIVACY ONLINE: A REPORT TO CONGRESS* 7-11, June 1998, *available at* http://www.ftc.gov/reports/privacy3/toc.htm.

22. *Id.*

information practices before collecting personal information from consumers;

(2) *Choice* - consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided;

(3) *Access* - consumers should be able to view and contest the accuracy and completeness of data collected about them; and

(4) *Security* - data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.[23]

The report also identified *Enforcement* - the use of a reliable mechanism to impose sanctions for noncompliance with these fair information practices - as a critical ingredient in any governmental or self-regulatory program to ensure privacy online.[24]

These Fair Data Principles have been echoed elsewhere. For example, the privacy principles of the Organization for Economic Cooperation and Development ("OECD"),[25] an international organization helping governments tackle the economic, social and governance challenges of a global economy, include:

Collection Limitation Principle - There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle - Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date.

Purpose Specification Principle - The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

---

23. *Id.*

24. *Id.*

25. OECD, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www1.oecd.org/dsti/sti/it/secur/prod/priv-en.htm.

> *Use Limitation Principle* - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except with the consent of the data subject or by the authority of law.
>
> *Security Safeguards Principle* - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
>
> *Openness Principle* - There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
>
> *Individual Participation Principle* - An individual should have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him, to have communicated to him, data relating to him within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him, to be given reasons if a request is denied, and to be able to challenge such denial, and to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
>
> *Accountability Principle* - A data controller should be accountable for complying with measures which give effect to the principles stated above.[26]

B. Application of the Fair Data Principles to CRM

Fair data practice concerns arise with CRM due to the fundamental nature of the CRM process: customer data from company-wide sources, together with other information both from within the company and from outside sources, are combined and analyzed to provide new insight into the best ways to market to and support the customer.

CRM vendors brag that their products can interrelate and retrieve customer and operational data from client computer systems and add relevant data and knowledge, and can provide

26. *Id.*

customer interaction solutions that encompass all forms of customer interaction.[27] As a result, a business's adoption of CRM software for gathering, using and storing information can impact all five fair data principles.

Notice is the essential starting point for a business that wishes to conform to the principles, and that notice should be given at the first point a customer or potential customer interacts with a part of the CRM system that can collect data. Any notice should be clear, understandable and conspicuous to the intended audience. Without notice that there will be data collection, and without an adequate explanation of what the data will be, the customer is entering a CRM system without the most basic knowledge of the business' intentions. That one-sided starting point is not likely to engender customer appreciation of and support for the CRM process.

Close behind the need for notice is the issue of choice. A business wanting to make effective and ethical use of CRM must give options to customers and potential customers as to whether they will permit personal information to be collected from them, and, if so, how much information and how that information may be used. This last point is especially important because consumers are quite likely to permit use of their personal data for the purposes of the inquiry or transaction in which they initially are asked for and give data. The difficulty arises when the business, using its CRM system to the fullest, wants to use those data for purposes other than the use for which the information was initially provided. This is the power of CRM: to assemble data that was put into the business for many original reasons, sort through those data for patterns and knowledge about customers, and use the data in new ways to market and support the customer. But if a customer does not know and agree that her data may be re-used within the company for purposes completely unrelated to the purpose for which she initially gave consent, she can say with justification under this fair data principle that she did not give informed consent for the secondary uses.

CRM magnifies the need for the access principle. As multiple

27. *See, e.g.*, Braun Consulting, *Capturing Customer Opportunities* (2002), *available at* http://www.braunconsult.com/solutions/sol_cust.htm; Buystream, *Buystream Merchant: Measure what Matters*, BUYSTREAM.COM, *at* http://www.buystream.com/display_page.asp?page_id=235 (last visited Feb. 6, 2002).

data points about a consumer are collected, processed and relied upon by a business to interact with that consumer, the probability of erroneous data increases. The access principle—that the subject of the data should be able to view and contest the accuracy and completeness of his data—is vitally important. Incorrect data not only may send the wrong message to a customer but may also cost the business in wasted sales activity. Providing an accessible vehicle for customers to view, challenge and correct data about themselves should make a significant difference, not only in customer satisfaction and acceptance, but also in the bottom line.

The need for security is also heightened by CRM. As a business accumulates more and more personal data about its customers, the effects of misused, abused or stolen data become more significant. Not only will customers object if their personal data is used within the company in ways they did not know of or choose to accept, if they find out that their data has that company fallen into the hands of third parties, they will certainly bring this violation to the attention of management and (in the more egregious cases) government.

This ties into the fifth principle, enforcement. The policy choice of the moment is whether businesses should be permitted, through industry groups or free-standing certification bodies, to self-police their privacy policies and actions, or whether government at one or more levels needs to provide and enforce at least a minimal set of standards.

IV. WHY SHOULD MANAGEMENT CARE ABOUT PRIVACY?

A reason often given for business reluctance to elevate privacy concerns is cost. Among the direct costs cited are the needs to hire executives or attorneys dedicated to privacy issues, to make privacy central to the business and dedicate increasingly more resources to privacy, to purchase new hardware and software to protect privacy, authenticate users, and secure databases containing personally identifiable information.[28] Industry sectors have also asserted that restricting their use of personally identifiable information will add costs to their products and services, particularly if "opt-in" requirements reduce their ability to share data and aggregate

28. Doug Brown, *Is Privacy Too Expensive?*, INTERACTIVE WK., Apr. 30, 2001, at 56.

personally identifiable information.[29] Financial services have estimated increased costs to consumers of $17 billion, while the Direct Marketing Association says that consumers would bear an additional $1 billion of costs.[30]

The most persuasive reason for managers of business adopting CRM to care about privacy is the potential for public embarrassment and financial exposure if privacy is forgotten or poorly handled. In the business-to-consumer setting, a business's deviation from a stated privacy policy can be pursued by the FTC as a deceptive practice, and state consumer laws give similar powers to states and private parties. At a business-to-business level, a stated privacy policy is likely to be viewed as a contract, with a breach actionable under state law.

In 2000, US Bank spent $3 million to settle a lawsuit brought by the Minnesota Attorney General's Office. That lawsuit accused US Bank of selling confidential customer financial data to a telemarketing firm, which targeted sales pitches at the bank's customers based upon that financial information.[31] Described as a "first of its kind" action, the Attorney General's complaint alleged that the disclosure of private, confidential information was in violation of US Bank's own stated privacy policy.[32] The settlement required the bank to stop sharing customers' financial information to market non-financial products, to give customers notice and an opportunity to "opt out" of the sale of their financial information to market financial products, and to provide refunds to some customers charged by telemarketers who bought their account numbers.[33]

The FTC has also been active in developing the law for online privacy issues. For example, on July 21, 2000, the FTC announced a settlement with the online retailer Toysmart.com (Toysmart) regarding alleged privacy policy violations.[34] Toysmart had collected personal information (names, e-mail addresses, ages,

29. *Id.*

30. *Id.* at 56-57.

31. Minnesota Attorney General, *Privacy Law Enforcement Efforts, at* http://www.ag.state.mn.us/consumer/privacy/Privacy_Law.htm (last visited Feb. 11, 2001).

32. *Id.*

33. *Id.*

34. Press Release, Federal Trade Commission, FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000), *available at* http://www.ftc.gov/opa/2000/07/toysmart2.htm.

billing information, shopping preferences, and family profiles) from children who visited the company's web site (allegedly without obtaining parents' consent for that collection) and from purchasers at the site.[35] Despite having told customers that their data would not be sold to third parties, when Toysmart went into bankruptcy, the company proposed selling the personal data as an asset of the bankruptcy estate.[36] The settlement prohibited Toysmart from selling the customer list as a stand-alone asset, and only allowed a sale of the data as a package which would have to include the entire web site, and then only to an entity in a related market that expressly agreed to abide by the terms of the Toysmart privacy statement.[37]

In addition to enforcement, the FTC has collected data about privacy policies in the online world, and reported to Congress on its findings.[38] In February 2000, the agency surveyed two groups of web sites. One was a random sample of 335 web sites, and the other group consisted of 91 of the 100 busiest sites on the web at that time.[39] The FTC found that over ninety-seven of the sites collected some type of personally identifying information from users, and that over 88% posted at least one privacy disclosure.[40] However, closer examination showed that only 20% of the "random" group and 42% the "most popular" met all four of the fair data principles (excluding enforcement).[41] Forty-one percent of the "random" group and 60% of the "most popular" group met both the notice and choice principles.[42]

In January 2002, Qwest Communications responded to a barrage of criticism over its plan to require customers to "opt out" of having their person information shared among Qwest-affilliated businesses. After prominent politicians, including a U.S. Senator, called for the plan to be converted to "opt in," Qwest withdrew the plan completely and said it would wait for the Federal Communications Commission ("FCC") to issue administrative rules

35. *Id.*
36. *Id.*
37. *Id.*.
38. *See* FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS, May 22 2000, 7-11, *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.
39. *Id.*
40. *Id.*
41. *Id.*
42. *Id.*

on the topic.[43] In that same press release, Qwest announced the appointment of a Chief Privacy Officer.[44]

V. OTHER LAWS ON PRIVACY WITH POTENTIAL CRM IMPACT

In addition to the general principles outlined above, there are now federal laws that add specific privacy standards to businesses operating in particular markets.

The Children's Online Privacy Protection Act of 1998[45] places restrictions on web sites which collect personally identifying information from children under thirteen. The FTC's rules implementing COPPA apply to any commercial web site or online service directed at children under thirteen that collects personal information from children, and to any general-audience web site where the operator has actual knowledge that it is collecting personal information from children.[46]

The Health Insurance Portability and Accountability Act ("HIPAA"),[47] and the Health and Human Services rules implementing HIPAA, adopt several of the Fair Data Principles by requiring notice to patients as to how their data will be used, how the data will be kept, and how the data will be disclosed; requiring that patients be offered a chance to see and amend their data records; and by requiring patient consent before their data is disclosed.[48]

For financial institutions, the Graham-Leach-Bliley Act[49] requires clear disclosure by all financial institutions of their privacy policies and an opportunity for customers to "opt-out" of sharing of personal information. Covered entities must also develop standards for safeguarding customer information.[50]

On the horizon, the National Association of Insurance

---

43. Press Release, Qwest Communications, Qwest Communications Withdraws Plan to Share Private Customer Account Information Within Company (Minnesota) (Jan. 28, 2002), *available at* http://www.qwest.com/about/media/pressroom/1,1720,900_archive,00.html.

44. *Id.*

45. 15 U.S.C. §§ 6501-6506 (2001).

46. 16 C.F.R. § 312 (2001).

47. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, Aug. 21, 1996.

48. *See* 45 C.F.R. § 160-164 (2001).

49. 15 U.S.C. § 1594 (2001).

50. 16 C.F.R. § 313 (2001).

Commissioners has developed a model act for state adoption which would cover not only financial information but also the sharing of health information that requires a specific authorization by the effected consumer.[51]

The FTC has vacillated over the need for new legislation for privacy in the online business world. In its July 2000 Report to Congress, the FTC concluded that industry self-regulation of privacy was not sufficient, and that legislation was needed to set basic standards.[52] The FTC recommended that Congress give the agency the power to establish rules, undertake enforcement, and establish safe harbors for self-regulation where appropriate.[53] However, under a new chairman in the Bush administration, the agency has done a turnaround and advised Congress that new legislation is not needed and that the FTC will instead focus on enforcement of existing statutes and education initiatives, increasing the resources dedicated to privacy protection by 50%.[54]

Finally, the European Union's (EU) 1998 Privacy Directive went into effect in July 2001. That Directive established a comprehensive regulatory scheme, under which only the information needed for a transaction can be gathered, and companies must explain why they will collect and use personally identifiable information, let individuals block information sharing with third parties, share personally identifiable information only with those third parties that also meet the "safe harbor" standards, give consumer access to their personally identifiable information, take reasonable precautions to make personal data secure, ensure that personal data collected is relevant for the purposes for which it is to be used, give individuals independent recourse for complaints, implement procedures for compliance, and remedy problems arising from noncompliance.[55] The Directive also applies to

---

51. National Association of Insurance Commissioners, *NAIC Privacy of Consumer Financial and Health Information Model Regulation*, Sept. 26, 2000, *available at* http://www.naic.org/1privacy/naic_privacy_publications.htm.

52. FTC, ONLINE PROFILING, A REPORT TO CONGRESS, Part 2, Recommendations, July 2000, *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.pdf.

53. *Id.*

54. FTC Press Release, *FTC Chairman Announces Aggressive, Pro-Consumer Privacy Agenda*, Oct. 4, 2001, *available at* http://www.ftc.gov/opa/2001/10/privacy.htm.

55. U.S. Dept. of Commerce, *Welcome to the Safe Harbor*, *at* http://www.export.gov/safeharbor/index.html (visited Feb. 11, 2002).

overseas companies that want to move data out of the EU.[56]

In an effort to assist American businesses, the U.S. Department of Commerce negotiated a "Safe Harbor" program with the EU, under which American companies can certify their compliance through the Department and avoid having to demonstrate compliance with each EU member.[57] The Safe Harbor agreement requires that organizations comply with the same seven principles as in the Directive: notice, choice, onward transfer, access, security, data integrity, and enforcement.[58]

The benefits of using the Safe Harbor approach include the following: all fifteen EU states are bound by the finding of adequacy; the U.S. participants get continued data flow from their affiliates or business partners in Europe; there are no EU requirements for prior approval of data transfers; and claims about problems with compliance will generally be heard in the U.S.[59]

As of July 2001, when the Directive became effective, only seventy-one U.S. companies had signed up under the Safe Harbor program.[60] As of the date of this article, the total was up to eighty-eight companies or groups.[61]

VI. CURRENT STATUS OF PRIVACY AMONG BUSINESSES

According to a survey of 100 security professionals involved in computer/Internet privacy security technologies or wireless access technologies, performed by the Sageza Group in the Fall of 2001, there is still a relatively low level of concern about liability issues arising from customer data collection.[62] The lowest level of concern was registered for the use of opt-in versus opt-out solutions on corporate web sites.[63] The highest levels of concern were reserved

56. *Id.*

57. U.S. Dept. of Commerce, *Safe Harbor Overview, at* http://www.export.gov/safeharbor/sh_overview.html (visited Feb. 11, 2002).

58. *Id.*

59. *Id.*

60. Ted Kemp, *Privacy Rules Cross the Pond,* INTERNETWK., July 16, 2001, at 1, *available at* http://www.internetweek.com/newslead01/lead071601.htm.

61. U.S. Dept. of Commerce, *Safe Harbor List, at* http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (last visited Feb. 11, 2002).

62. George V. Hume, *Hard Line on Security is the Only Way for E-Markets: Exchanges must assure customers that their data is safe and won't be shared,* INFORMATION WK., Oct. 29, 2001, at 83, *available at* http://www.informationweek.com/834/security.htm.

63. *Id.*

for protecting electronically gathered and stored customer data, and having other companies access a corporate intranet.[64]

Perhaps more surprising was that same survey's finding that 58% of the security professionals either "agreed somewhat" or "agreed strongly" that the government should require Web sites that collect personal data to comply with minimal privacy guidelines.[65] Only 19% of those security professionals believed that industry privacy-seal programs were providing sufficient privacy protection.[66]

There seem to be tentative movements by businesses using CRM to factor customer demands for privacy into their adoption of the technology. The Minneapolis Star Tribune, for example, had moved in Spring 2001 to a transactional database and CRM system that would permit the daily newspaper to avoid sending e-mails to subscribers who had opted out of such e-mails.[67] CRM vendors have announced products that add systems of software-based rules to act as sophisticated filters between the CRM database and the portion of the software that actually sends out e-mails.[68] Those rules permit accommodation of a wide range of customer preferences, ranging from complete opt-outs to requests for communication in specific forms, at particular locations, or only upon the occurrence of pre-arranged events.[69]

Despite the attention being given to the privacy issue in the mainstream press and within the business community, overall response levels remain low. According to a survey of 249 businesses by InformationWeek Research in the Summer of 2001, only the healthcare and financial services sectors reported that 75% or more had a publicly displayed privacy policy.[70] Business services reported 75% had a posted policy, while retail was under 45% and manufacturing was under 35%.[71] Given that notice is one of the simplest of the Fair Data Principles, these results suggest that many industry sectors have far to go in meeting even the most basic

64. *Id.*
65. *Id.*
66. *Id.*
67. Kemp, *supra* note 17, at 15.
68. *Id.*
69. *Id.*
70. Helen D'Antoni, *Companies Struggle With Data Classification,* INFORMATION WK., Aug. 20, 2001, at 33, *available at* http://www.informationweek.com/story/IWK20010817S0007.
71. *Id.*

portions of the Fair Data Principles.

In Europe, the Commission responsible for enforcing the Data Directive has acknowledged that enforcement will be difficult, due to limited staff, but has indicated they will respond to complaints.[72] The International Chamber of Commerce has asked the Commission to approve alternative language for international contracts that would safeguard data moving out of the EU without using the standard contract clauses adopted by the Commission. The Chamber's request stated the following:

> [T]he [filing] groups believe that, as recognised in the Commission's decision of June 18, 2001 recognising a set of standard contractual clauses, there should be a variety of clauses available for use by business. If approved, use of the Clauses would provide a simple, inexpensive legal basis under the European Data Protection Directive for transferring personal data from any EU Member State to data controllers in third countries, without the necessity of having the Clauses approved by national data protection authorities. The Clauses are designed to co-exist with the standard contractual clauses approved by the Commission on June 18, and are limited in scope to controller-to-controller transfers. The Clauses provide a flexible alternative to the clauses already approved which better reflect the global business realities of data transfers, while still offering just as high a level of data protection.[73]

VII. CONCLUSIONS AND RECOMMENDATIONS

While working within the Fair Data Practices would be a sound ethical decision by almost any business, for an organization contemplating use of CRM, adoption of the Principles is virtually essential to avoid both customer backlashes and unwanted oversight from regulators. If planned as part of a CRM adoption process, and included in the cost analysis of CRM implementation, an upgraded commitment to privacy need not be a budgetary

72. Juliana Gruenwald, *Safe Harbor, Stormy Weather,* INTERACTIVE WK., Oct. 30, 2000, at 32.

73. Policy Statement, International Chamber of Commerce, Proposed Standard Contractual Clauses for the Transfer of Personal Data from the EU to Third Countries, (Sept. 17, 2001), *available at* http://www.iccwbo.org/home/statements_rules/statements/2001/contractual_clauses_for_transfer.asp (emphasis added).

problem. Rather, a top-down commitment to the Principles can result in lower ongoing costs of customer relations and regulatory compliance.

An emerging concept for businesses committed to effective e-commerce is that of a Chief Privacy Officer ("CPO"). Such a CPO would typically be responsible for training employees about privacy, comparing privacy policies with potential risk, managing a customer-privacy dispute and verification process, and advising senior management. Industry analysts who advocate a CPO position recommend that a company appoint a CPO with a privacy team to draw together the needed types and depths of expertise: legal, IT, PR, and marketing. They advise companies to give that CPO appropriate authority internally to hunt down and fix compliance problems. At the same time, they recommend against making the privacy team a bottleneck for the overall sales and customer support efforts of the enterprise, and suggest that organizations create an enterprise-wide privacy policy, craft an external policy statement, and keep the promises made in that statement.[74]

Given the certainty of continued government interest in privacy, and the likelihood of additional forms of government control (either through industry-specific programs or overall privacy policy), the time to invest in effective privacy policy development and implementation is at the very start of CRM planning, not after the first disaster caused by a lack of such a policy in a CRM-enhanced business environment.

74. *See* Kelley, *supra* note 12.