Clients' Views on Privacy and Security After September 11: Have They Changed? Should They? An Information Technology Lawyer's Perspective

by
*Richard G. Lyon**

Good morning. My name is Richard Lyon, and I am with the Dallas office of Gibson Dunn & Crutcher, a mega-firm with 750 lawyers in eleven offices in the United States and Europe. As you probably know, but can certainly ascertain from the title of my presentation, our practice and the firm's practice serve mainly corporate clients. My personal practice in recent years has focused on intellectual property and information technology (IT) based transactions: the acquisition, protection, and exploitation of intellectual property rights, and the acquisition or provision of information technology services. One of our clients in these areas, incidentally, is Southern Methodist University.

Typical of lawyers, I begin my presentation with a disclaimer. When I refer to clients, I base my comments on my own clients and clients of my firm, friends and colleagues who are employed by IT service providers or in-house technology groups. There was nothing scientific about the survey—it wasn't a survey at all, rather, arbitrary questions to arbitrarily selected individuals. This presentation is laced with personal opinions: my own and those of the outsourcing professionals, technology officers, and IT professionals with whom I spoke. I believe, however, that the concerns and priorities of these individuals—who include individuals from large and small companies, IT providers, and users—provide a fair representation of current corporate priorities on privacy and security.

Less than two weeks after September 11, 2001, I attended a program on digital commerce and the Internet held at the headquarters of the World Intellectual Property Organization in Geneva. I distinctly recall the presenter on privacy, who spoke by videoconference from Washington, D.C. She had been scheduled to speak about the state of privacy and privacy initiatives on Capitol Hill. Following September 11, however, she said that she changed her presentation completely because, she said, privacy was "in the icebox." The overarching and single-minded concern of Congress was security. She

---

* Richard G. Lyon is Of Counsel at the Dallas office of Gibson, Dunn & Crutcher LLP. Ellen Ratliff, an associate attorney at Gibson, Dunn & Crutcher LLP in Dallas, assisted in the preparation of this speech, which was given at the Computer Law Review & Technology Journal's first symposium on April 3, 2003.

then began a discussion of what was later to become that inappropriately named piece of legislation, the USA Patriot Act.[1]

In fact, in the years immediately prior to September 11, 2001, personal privacy and the protection of electronically-stored personal information had been subjects actively addressed by Congress and state legislatures. With respect to protection of personal information stored by the government or private parties, cursory research revealed ten statutes (in addition to HIPAA,[2] which I will discuss in more detail later) with provisions addressing this subject, and in most cases limiting the use to which collective data could be put:

- Electronic Funds Transfer Act,[3] governing financial records;
- Privacy Act of 1974,[4] regarding government use of personal data;
- National Espionage Act of 1996,[5] Computer Fraud and Abuse Act,[6] and Cable Subscriber Privacy Act,[7] each governing access to and use of electronic communications and stored data;
- Cable Communication Policy Act;[8]
- Drivers Privacy Protection Act;[9]
- Right to Financial Privacy Act;[10]
- Telephone Consumer Protection Act;[11]
- Video Privacy Protection Act.[12]

With respect to another side of personal privacy, once aptly described by Justice Brandeis as the right to be left alone,[13] state legislatures especially have been—and continue to be—active in addressing uninvited and un-

1. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
2. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended at 42 U.S.C. §§ 1320d - 1320d(8) (2000)).
3. 15 U.S.C. § 1693 *et seq*. (2000).
4. 5 U.S.C. § 552a (2000).
5. Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (1996) (codified as amended at 18 U.S.C. §§ 1831-1839 (2000)).
6. 18 U.S.C. § 1030 (2000).
7. 47 U.S.C. § 551 (2000).
8. *Id*.
9. 18 U.S.C. § 2721 (2000).
10. 12 U.S.C. § 3401 (2000).
11. 47 U.S.C. § 227 (2000).
12. 18 U.S.C. § 2710 (2000).
13. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

wanted communication, most notably "no call" lists[14] to limit uninvited telephone solicitations and anti-spam e-mail legislation to cut back on uninvited electronic communications.[15] As I will mention later, spam e-mail continues to be a serious problem, not only for those of us who receive on a daily basis invitations to increase the size or functionality of various body parts, advertisements for cleaning septic tanks, and once-in-a-lifetime investment opportunities, but also for network managers who are concerned about spam overwhelming the capacity of their systems.

You have heard today from the United States Attorney that data security and counter-terrorism are and will remain very high priorities of the government. You'll hear this afternoon from the American Civil Liberties Union that citizens' privacy, indeed constitutional protections, have been forgotten or, worse, knowingly sacrificed in the name of national security. Yet I believe that our governments have not lost sight of citizens' calls for protection of privacy and protection against unauthorized use of personal information. Governments have not ignored the pressure for the privacy that the Internet age necessarily generates.

Is there reason for concern? Of course there is. Technology and the exploding use of the Internet as a business medium, by their nature, make personal information easily accessible to businesses, financial institutions, government, and private individuals and organizations. Perhaps the post-September 11 emphasis on security has made us forget momentarily the simple fact that greater access is a necessary—I repeat, necessary—consequence of the convenience, efficiencies, and many other benefits that e-commerce undeniably provides; what the marketplace now demands; and what all of us are beginning to take for granted. We could easily spend an entire conference discussing the philosophical question of just what a fully informed consumer would willingly trade in return for the convenience, vastly increased accessibility to information of all kinds, and saving of time that are returned for this small payment. I believe that most people's answer would surprise civil libertarians like myself.

Yes, there is reason to worry. But I believe that my colleague who spoke in September 2001 may have overvalued the mood of that moment, for she has been proven wrong when it comes to privacy concerns of corporate America in the last twenty months. For reasons you may guess from the title of this presentation, I deliberately do not use the word *reaction*, since the

14. *See* TEX. BUS. & COM. CODE ANN. §§ 43.101-43.104 (Vernon 2002). The Federal Trade commission has promised that a national no-call list will be forthcoming. *See* "The National Do Not Call Registry – Amendment to the Telemarketing Sales Rule," *available at* http://www.ftc.gov/bcp/conline/edcams/donotcall/index.html (last visited Oct. 9, 2003).

15. The harshest of these (as yet) is Virginia's criminal statute, VA. CODE ANN. §§ 18.2-152.2, 18.2-152.4, 18.2-152.12 (Michie 2002). For an example of a law imposing civil penalties, see CAL. BUS. & PROF. CODE §§ 17538.4, 17538.45 (West 2003).

drivers for the heightened awareness of privacy are not a reaction to September 11. Privacy concerns are high on the issues list of chief information and chief technology officers and marketers as well. I shall mention the motives stated to me for these concerns. It is not just complying with the law, though that certainly plays a part. Many in corporate America recognize that personal information about individuals is a valuable asset, but only if it is properly guarded. Since most customers value their privacy and resent someone else selling their personal information for profit, it is good business to be careful.

I will now turn to some specific government directives that have directed my firm's clients to safeguard personal information about their employees and customers. As noted above, some of this information is industry-specific, particularly in regard to the financial industry. The Graham-Leach-Blily Act[16] and the Fair Credit Reporting Act,[17] while not all that certain privacy advocates desire, do impose legal duties on financial institutions and users of financial information to maintain personal information in confidence and to limit its use for purposes other than that for which it was obtained. These statutes also give individuals the right of access, and more, to their personal information. Perhaps not all that could be done, but it is a good start.

Other legislation, motivated more by political hot buttons than a concern for privacy, nevertheless provides evidence that the government recognizes that the unfettered use of personal information should be prohibited. In addition to its better-known and similarly acronymed cousin, the Child Online Protection Act ("COPA"),[18] the Children's Online Privacy Protection Act ("COPPA")[19] limits the collection and use of personal information from and about "children" (defined as persons under the age of 13) by generally requiring demonstrable parental consent for such collection. The Federal Trade Commission ("FTC") is the enforcer of COPPA, and its rules[20] take an expansive view of the statutory language. For example, the FTC has taken the position in litigation that by asking for date of birth in an electronic questionnaire, a website operator may knowingly be targeting children.[21] The operator of a commercial website that is directed to children or knowingly provides access to children under 13 must obtain parental consent through

16. Gramm-Leach-Billey Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended at 12 U.S.C. § 1811 (2000)).

17. 15 U.S.C. § 1681 *et seq*. (2000).

18. 47 U.S.C. § 231 *et seq*. (2000).

19. 15 U.S.C. § 6501 *et seq*. (2000).

20. FTC Children's Online Privacy Protection Rule, 16 C.F.R. § 312.1 *et seq*. (2000).

21. Federal Trade Commission Staff Report, FTC Protecting Children's Privacy Online (April 2002) *available at* http://www.ftc.gov/os/2002/04/coppasurvey.pdf (last visited Oct. 9, 2003).

one of several means, such as a faxed signature, a digital signature, or a valid credit card used in the transaction. Today, e-mail approval will suffice, but the Act and its rules contemplate ending that option.[22] Last year's settlement with Etch-A-Sketch[23] and warning letters to more than 50 children's sites indicate the Commission's intent to enforce this statute in more than a nominal manner. The FTC survey on compliance, a staff report released in April of last year, indicated that less than 10% of websites collecting information from children even had a published privacy policy—an astonishing statistic.[24] I strongly suspect that number has risen dramatically.

The government action that has by far been most urgent and influential on private industry directly targeted the maintenance of confidentiality and accuracy of personal information. The three government initiatives most often cited by IT professionals as the reason for an increased sensitivity to the privacy of personal information are the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[25] the European Union ("EU") Privacy Directive,[26] and the need for a privacy policy.

The HIPAA privacy rules, by the way, are the result of a somewhat unusual legislative twist. HIPAA was enacted in August 1996. The statute provided that if Congress failed to pass national medical privacy legislation by the end of August 1999, the Department of Health and Human Services ("HHS") was directed to issue regulation on the subject. Congress didn't act, so HHS did.[27] The result is the Privacy Rules. It will be interesting to see if Congress awakens to its own action after the impact of these rules is seen.

HIPAA compliance is a topic for any business that provides either benefits or health insurance to its employees, which of course means most businesses. This is a timely symposium, since the week after next, April 14, is the deadline for most health plans' compliance with HIPAA's privacy rules. I am, happily, not a HIPAA expert. For those of you who have another year to comply—or those of you who are worried about liability after April 14—I can certainly point you to two of my Dallas colleagues who are. For pur-

22. Children's Online Privacy Protection Rule, 67 Fed. Reg. 18818 (2002) (to be codified at 16 C.F.R. § 312).

23. FEDERAL TRADE COMMISSION STAFF REPORT, *supra* note 21.

24. *Id.*

25. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended at 42 U.S.C. §§ 1320d - 1320d(8) (2000)).

26. Council Directive 95/46/EC, of the European Parliament and of the Council, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, (Nov. 1995) *available at* http://www.datenschutz-berlin.de/gesetze/europa/den.htm (last visited on Oct. 9, 2003).

27. Dept. of Health & Human Services, Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. §§ 160-164 (1999).

poses of today's session, I shall list the aspects of corporate operations that HHS Privacy Rules thereunder will impact.

The Privacy Rules require special handling, in particular strict rules for maintaining privacy, of "protected health information"—"PHI" in the alphabet soup of the employee benefits world. PHI is individually identifiable health information, in any form, including oral information, that is created by a covered entity. While employers are not technically covered entities, their health plans usually are. Compliance with HIPAA will require (or has already required) covered entities and the employers that manage them:

- to amend the plans themselves to bring them into compliance;
- to appoint a privacy officer whose duties, among others, include serving as a person to receive complaints from individuals covered by the plan;
- to send a notice to all plan participants (i.e., all employees) of assorted rights under the privacy policy that the plan must adopt. These rights include the right to file a complaint with the privacy officer or HHS. Any material change in a plan's PHI policies requires a new notice;
- to train all employees who will handle PHI on the importance of compliance and the procedures the plans adopt;
- to take sanctions against employees who fail to comply with the plan's rules;
- to establish and maintain extensive documentation and document retention policies including an individual's right to review his or her PHI and request amendments;
- to deal with a covered individual's "personal representative" (I assume that this includes lawyers); and
- to provide in all contracts with "business associates" requiring the business associates to comply with the plan's compliance procedures. A business associate is any one person or entity to which administration of the plan, including payment of claims, is entrusted.[28]

The European Union's privacy directive is an excellent illustration of one of the obvious commercial consequences of the Internet and electronic commerce. International commerce is now the ordinary course of business, especially for transactions in services, software, and anything else that can be transmitted digitally. With the ubiquity of the Internet and the intangible nature of software, the smallest startup company—even an individual—can easily become an international seller. I do not limit this comment just to the selling or licensing of software. Software programs that all of us use on a daily basis allow a citizen of Bulgaria, for example, to purchase a product made and sold in Dallas just as easily as anyone in this room.

28. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended at 42 U.S.C. §§ 1320d - 1320d(8) (2000)).

The EU Directive, adopted in 1995,[29] appears to be as robust as ever after September 11. The EU Directive applies to the processing of any individual's personal data, with both terms very broadly defined. *Processing* includes any operation or set of operations that is performed on personal data, by automatic means or otherwise;[30] *personal data* includes any information relating to an identified or identifiable person.[31] As is true with HIPAA, the intent and purpose of the EU Directive is the protection of personal information. Processing of personal data is allowed only:

- with the subject's consent (and consent, of course, means informed consent);
- if the processing is necessary for performance of the contract to which the subject is a party or to take action requested by the subject;
- if the processing is necessary for compliance with a legal obligation;
- if the processing is necessary to protect the "vital interests" of the data subject;
- if the processing is necessary for the performance of a task carried out in the public interest; or
- if the processing is necessary for legitimate interests of the data controller, unless those interests are overridden by the interests for fundamental rights and freedoms of the subject.[32]

The EU Directive is directly pertinent to United States businesses because it prohibits the transfer of personal information outside the European Union to any jurisdiction that does not ensure an "adequate" level of protection for personal data.[33] Although the EU has not yet deemed U.S. laws "adequate" in this regard, the United States government has worked with the EU to negotiate a safe harbor.[34] The safe harbor requires companies and organizations that wish to benefit from the program to implement a privacy regime including at least:

- notice of the purposes for which the information is collected and the uses to which it will be put, including the types of third parties to which such information will be disclosed;
- a right to opt out of disclosures to third parties or uses to which personal information will be put; where "sensitive data" are at issue, an explicit choice to opt-in to third-party disclosure (since it is not always clear what is "sensitive," our advice to clients generally is to provide opt-in for all information);

29. Council Directive 95/46/EC, *supra* note 26.

30. *Id.*

31. *Id*.

32. *Id*.

33. *Id*.

34. DEPT. OF COMMERCE, SAFE HARBOR OVERVIEW, *available at* http://www.export.gov/safeharbor/sh_overview.html (last visited on Oct. 9, 2003).

- limiting outside disclosure to third parties that have accepted the notice and choice provisions stated above and which will honor the privacy provisions of the Directive;
- reasonable precautions to protect stored and transmitted data from loss, misuse, or unauthorized access or disclosure, and to maintain the integrity of the data collected;
- the subject's right of access to the data, and means to correct, amend, or delete it; and
- mechanisms for insuring compliance with these principles.[35]

The EU Directive raises the interesting issue of how international privacy standards (or at least standards among industrialized countries) may develop. I have recently been working with a start-up company that licenses software in Europe and Asia as well as the United States. The client posed the question of whether compliance with the EU Directive would place its privacy policy within the current requirements for North America and Asia. Almost certainly it would mean compliance in the United States. Simply to avoid the confusion and expense of separate compliance polices for different data bases, actual corporate practice, if not a formal standard, may well migrate to what in this instance is the highest, not the lowest, common denominator—at least until that bar is raised to a compliance level deemed to be acceptable by the business community.

Privacy policies illustrate another obvious consequence of Internet commerce: today Internet commerce *is* commerce, and vice versa. What business that sells to consumers—indeed any business at all—does not have a website? And every one of these website operators routinely obtains personal information from their customers and prospective customers and uses that data to meet these individuals' immediate requests for goods, services, or information, and for future marketing to these persons and others. Obvious examples are eBay and Amazon.com. Less obvious, but equally apt, examples are Neiman Marcus and SMU's alumni office.

At the risk of defaming some of my firm's own clients, I will state unequivocally that any commercial website operator, large or small, that does not maintain, display prominently, and enforce a privacy policy for information obtained through its website is a fool. A simple checklist for the privacy policy should contain at least the following:[36]

- Make it clear that the user must opt-in or may opt-out. Unlike the EU, neither is required; and
- Explain what information is collected and how, its intended uses, and its likely recipients.
- If the data will be disclosed to third parties, state this expressly and describe the third parties and the purpose of the disclosure;

35. *Id.*

36. You will note its similarity to the punch list for compliance with the EU Directive and related U.S. Safe Harbor.

- Explain that a user may avoid entering requested information and may disable cookies. If this will degrade website operation for a particular transaction (or future transaction), make that clear;
- Explain to what extent consumers can view the information collected about them;
- Explain the steps taken to secure personal information, both in communications and while stored;
- Provide a means for individuals to ask questions or register complaints concerning the collection or use of personal information;
- Require third parties to whom information is disclosed to agree—by contract, in writing—to obey the privacy principles of the website operator with respect to the data transmitted to them; and
- Reserve the right to update or alter the privacy policy at any time, by appropriate notice on the website.

I will add three other principles that I include in my advice to corporations implementing a website:

- First, keep it simple. I often use the words "idiot proof;"
- Write it clearly, in everyday English; and
- Most importantly, do what you promise.

FTC enforcement actions have seized upon broken promises rather than inadequate data protection or breadth of a policy itself. For example, in the *Toysmart* settlement,[37] Toysmart had included in its privacy policy that it would "never" disclose personal information in its database to third parties. Toysmart filed for bankruptcy protection and, as debtor in possession, sought to sell its business. One of the items made available by the company to prospective buyers was the customer database. To a corporate lawyer, this seems entirely reasonable, certainly consistent with the debtor-in-possession's legal obligation to get the most for its creditors. The FTC took the view that "never" meant *never*. Under a consent judgment with the Commission, Toysmart agreed not to sell the database as a standalone asset and only to disclose it to a buyer of its entire business, when approved by the bankruptcy court. After objection by several states' attorneys general that this inadequately protected personal information of their citizens, the sale was not approved. Later, a corporate affiliate of Toysmart purchased the database for the express purpose of destroying it. It is noteworthy that FTC proceeded under Section 5 of the Federal Trade Commission Act,[38] which prohibits any "deceptive practice"—an extraordinarily broad and subjective standard.

I hope it is clear from these three examples that legal compliance alone has kept corporate IT personnel sharply focused on privacy on a daily basis.

37. The Complaint, the First Amended Complaint, the Stipulated Consent Agreement and additional documents in FTC v. Toysmart.com LLC, 2000 WL 1523287 (D. Mass. Aug. 21, 2000) *available at* http://www.ftc.gov/opa/2000/07/toysmart2.htm (last visited on Oct. 9, 2003).

38. 15 U.S.C. § 45 (2000).

What are the motivators? Certainly compliance with the law for its own sake is important. Businesses want to be good corporate citizens. A second and ever-present motivator is the avoidance of liability. Liability doesn't just mean legal liability, but that can be important.

HIPAA does not provide a private right of action for violation (indeed, it is difficult to see how it could, since the Privacy Rules are the product of agency action, not legislation). Unlike ERISA,[39] however, the Act itself does not preempt applicable state law, and more than a few states (though not, as yet, Texas) have, by constitution, statute, or judicial decisions, recognized a cause of action for invasion of privacy that clearly applies to unauthorized disclosure of personal information kept in a database. For instance, Doubleclick obtained summary judgment dismissing many federal claims against it;[40] however, it failed to do so in a California state court.[41] The Privacy Rules will surely be used as a standard of care in any case brought to redress injury, actual or perceived, which follows improper disclosure of PHI. Think of the mental anguish!

Moreover, this is the land of punitive damages and the class action, words that strike dread in the heart of legal and financial professionals. Somewhat surprisingly to me, there have been few reported cases, and no blockbuster verdicts or settlements, involving sale of personal data, but it's still early days yet. Besides, even without class certification or punitive damages, it is not difficult to calculate actual, direct damages to a business's customers whose credit card information is taken from that business's database.

Far more devastating than a federal fine or class action settlement is the terrible publicity and attendant loss of business and damage to business reputation that inevitably accompany any prominent unauthorized release of personal information. The Doubleclick settlement that I mentioned earlier and the recent confession by the University of Texas[42] glaringly illustrate this proposition. Information technology professionals and their corporate clients are hard at work to avoid becoming this kind of front-page news.

But the best motivator of all is recognition that information about customers is a very valuable corporate asset, and that it remains valuable only so long as it is kept secret. I do not say this in the sense of a commodity that can be sold or otherwise directly exploited as a commodity, although some

39. Employee Retirement Income Security Act of 1974, 29 U.S.C. §§ 1001 *et seq*. (2000).

40. *In re Doubleclick, Inc. Privacy Litig*., 154 F. Supp. 2d 497, 527 (S.D.N.Y. 2001).

41. *In re Doubleclick Cases*, No. JC4120, 2001 WL 1029646, at *1 (Cal. Super. Ct. Jun. 11, 2001).

42. Joshua Benton, *UT Case Shows Risk of Using Social Security for ID Information of 55,000 People Stolen in Database Hacking*, THE DALLAS MORNING NEWS, March 7, 2003, at 1A.

companies have tried to do so. Knowing the buying habits of a business's customers and prospective customers enables that business to serve those people better, making them even better customers, and to leverage the satisfied customers and the goodwill that they generate into new products, better services, and desired innovations. It is an acknowledgement that customers are the most important asset of any business, surely of any successful business.

This brings me to one thing that has changed since September 11 on the agenda of the prudent IT professional: security. September 11 translated this from merely a strategic concern, a hypothetical on everyone's checklist, to an everyday, day-to-day issue. This is particularly true with respect to data stored electronically and the technology used to store and access it. That is so for several reasons. First, more and more data are accessed and stored electronically rather than in hard copy. Second, while the information is not any more important now, it surely is much easier to access and to steal. No longer does the industrial spy take a photograph of every page of sensitive information or even make photocopies and smuggle them out in his briefcase. Today an entire database can leave corporate headquarters in one personal computer or from a single click on a button on a personal computer.

A substantial part of an IT professional's responsibilities is security of all kinds. The more traditional lock and key physical security remains important. Access to office premises, data storage facilities, and any sensitive information is routinely restricted also by access code, radio frequency, and other electronic means of identification.

Network security is becoming ever more sophisticated. I can remember when only a few website operators offered "secure" sites for consumer transactions done with a credit card. Now it is routine. Encryption, even for personal devices like my Blackberry, is commonplace. September 11 has broadened the scope of likely wrongdoers to include people who want to crack the code to do real harm. The relatively open e-mail systems that most of us use are vulnerable to invasion by unscrupulous parties. Until now, the ones we've read about have been done by super-geeks, individuals whose objective is the satisfaction of outwitting the pros by, say, developing a virus or other invading creature that gets through the firewall. Who knows what will happen if the next such invader comes from a criminal syndicate intent on stealing hard cash, or from a terrorist organization bent on disrupting commerce, a particular organization, or everyday life. Businesses have routinely turned to greater use of and more sophisticated techniques for encryption on what used to be routine data.

While not usually considered a security issue, spam is definitely an increasing problem in terms of interference with the uses for which businesses intend their data networks. One client cited statistics in support of a prediction that, unless somehow contained, spam will overwhelm businesses' e-mail systems in the next two or three years. States and the federal government are undertaking studies and considering legislation addressing e-mail

spam. And it will be a wealthy man or woman who develops a foolproof anti-spam filter of broad application.

September 11 has converted disaster recovery plans from an afterthought, usually meant for a natural disaster such as an ice storm or hurricane, to a very serious undertaking intended to address a deliberate attempt to destroy. Data back-up is now more than a routine. In designing an IT system, clients pay real attention to redundancy features. Clients are making real plans for a "code red" contingency, when a vast data network may need to be operated and supported by individuals working from many different locations, none of them company premises.

As you might expect, more and more clients are looking to the experts to devise and implement heightened security measures. In addition to the true security consultants, companies are taking advantage of professional services as a security measure. There is an increasing belief that an "outsourcer" will be able to keep current with the times in technology, not just for the provision of services, but also to comply with government directives on privacy and with contingency planning. Application service providers, traditional IT outsourcing, outsourcing of decision-making business processes, and making use of third party facilities for data centers and databases are a clear trend, in no small part security-driven.

What does all of this mean in terms of privacy? In my view, the mere fact that privacy and security were on the wish list of every chief technology officer with whom I spoke indicates that business is more keenly attuned to the protection of personal information than at any time during my career. Clients are putting their money where their mouth is, too. At a time when business is stagnant, and budgets (information technology budgets, too) pared to the bone, clients are spending more than ever before to protect their data, including personal information. Whatever the motive, privacy is a current and important topic of concern for corporate America.