BNA, INC.

PRIVACY & SECURITY LAW

VOL. 3, NO. 3 PAGES 51-78 REPORT JANUARY 19, 2004

Analysis&Perspective

PrivacyLegislation

Fifteen new privacy laws were passed by California in 2003, covering topics ranging from financial information to spam, identity theft, marketing restrictions for health information, and obligations in the event of an information security breach. The author explores the impact the laws could have outside California and says the most lasting result of the California experience in 2003 may be to reinvigorate privacy as a subject that will generate new debate and new regulations.

What's Up With California?

BY KIRK J. NAHRA

California was in the news a lot in 2003. The recall election captured the attention of newswatchers around the country. Earthquakes and wildfires also could be seen regularly on the nightly news. But for those involved in the law of privacy, California had a much more important impact in 2003—one that applies to businesses across the country and will affect substantial commercial activity in 2004 and in the future.

Kirk J. Nahra is a partner with the Washington, D.C., law firm of Wiley Rein & Fielding LLP, where he represents a wide range of insurers, health plans, and others on issues related to the privacy and security of information. He is the editor of Privacy Officers Adviser, a monthly privacy newsletter of the International Association of Privacy Professionals. He can be reached at 202.719.7335 or Knahra@wrf.com

California in 2003

Joanne McNab, chief of the California Office of Privacy Protection, has spoken widely about the substantial privacy activity in California in 2003—focusing on the *15* new privacy laws passed by California in 2003, covering topics ranging from financial information to spam, identity theft, marketing restrictions for health information, and obligations in the event of an information security breach.

Enactment of 15 new privacy laws in one year is astonishing—and doesn't even count other recent California laws, such as the 2001 law on use of Social Security numbers (SSN) that started a trend in which at least seven other states passed such laws in 2003, with more states certain to follow in 2004.

What is going on in California? Why all this activity at once? Is it making any difference? How is it affecting privacy legislation in other places? And does this flood of activity make any sense?

What Are Some of the Major Laws?

♦ *SB 1—Financial Privacy*

This law, regulating the information-sharing practices of financial services companies, is the culmination of several years of debate in California following passage of the federal Gramm-Leach-Bliley

  PVLR ISSN 1538-3423

(GLB) Act. After several failed bills, and initiation of a referendum that would have been tougher on financial services companies than any of the proposed legislation, the California legislature adopted SB 1 this year, creating an ''opt-in'' mechanism for information sharing with nonaffiliated third parties, and an ''opt-out'' mechanism for affiliate information sharing (both more ''stringent'' than the GLB standard).

♦ *Security Breaches*

The California legislature also passed a law requiring consumer notification in the event of security breaches involving certain personal information posing a high risk of identity theft. The law itself is fairly specific on the steps that a company must take if there is a breach—and the California Office of Privacy Protection has increased the potential scope of the law through issuance of a series of ''best practices'' that likely will significantly affect how a company's actions following a breach are evaluated in California.

♦ *AB 68—Online Privacy*

This law mandates that all Web sites must have a privacy policy and must comply with it (creating far broader obligations than any federal law related to Web sites).

♦ *SB 186—Spam Legislation*

This broad statute prohibits the sending of spam to or from a California e-mail address without direct consent of the individual.

Other Laws

This is just a partial list of issues being addressed in California. Other laws this year include regulation of consumer rights as to personal information held by non-financial institutions, restrictions on disclosure of health information for marketing, and prohibitions on visible mailing of Social Security numbers (in situations where other California law allows the mailing of a SSN at all).

And the state is not done. When recent news reports publicized that a California hospital had contracted certain medical transcription work to a Texas company, which subcontracted to an entity in Pakistan, and the Pakistani concern threatened to post certain patient health information on the Internet, a California legislator rushed into this untapped area to introduce legislation to ban sending medical data to contractors abroad.

Who Should Care?

So, who cares about all of this California activity? It might be easy to dismiss this flurry of legislative activity as simply ''it's California''—but that is far too simple. Initially, most companies that have consumer information, regardless of where they are located, will be directly affected by these California laws, in terms of facing exposure from California regulators, the California Attorney General, or private parties with the ability to bring statutory causes of action.

What are the key issues for companies to consider in evaluating their own exposure to these laws?

♦ *Geographic Scope*

Most of these California laws apply to ''any person'' (or some other subgroup of companies, such as financial institutions) who has information on California residents. Therefore, it may not matter where the company is based or whether it has any particular focus on California. SB 1, for example, applies to any financial institution that has personal information about a California resident. The security breach law applies to any company that has a security breach involving certain information of a California resident. So, understanding your customer base is critical, and that may be particularly difficult in some situations. For example, the antispam law—as passed (and subject to preemption as discussed below)—applies to e-mail addresses of California consumers (how do you tell where knahra@aol.com lives?).

♦ *Private Cause of Action*

Some of the statutes create a private cause of action, in addition to specific governmental enforcement jurisdiction. The California Social Security number law allows for private suits as part of the ''unfair competition'' law. Under the security breach law, there is a private suit for any consumer injured by a violation of the law— and the consumer may recover damages as well as seek an injunction.

♦ *Enforcement*

Understanding how these laws will be enforced is also important. Obviously, large California companies with visible California customer bases are more substantial targets of enforcement efforts. But under many of these laws, the defendant in a California enforcement action need not be a California company. The financial institutions laws, for example, are not limited to entities licensed in California. Most of the laws apply to ''any person'' who has the relevant information. SB 1 allows for civil penalties of $2,500 per violation, with enforcement actions brought by the California attorney general or the relevant ''functional regulator.''

Broader Effects on the Privacy Debate

Next, beyond their direct effect, California's actions will affect the overall privacy debate. The California Social Security number legislation, passed in 2001, has already led to passage of similar legislation in at least six other states (Arizona, Connecticut, Georgia, Missouri, Texas and Utah), with legislative proposals in at least 12 other states (with more to follow in 2004). SB 1 led to a spirited debate in Congress (in the otherwise unconnected consideration of the Fair Credit Reporting Act). As a result, although important parts of the California legislation have been preempted, more detailed provisions on certain information sharing by financial institutions have been enacted and a revived debate on overall financial privacy may reappear in 2004. The California spam law led directly

PVLR ISSN 1538-3423

to passage by Congress of the new federal spam statute. So, lots of people are paying attention to California, and the California laws are, at a minimum, stimulating and influencing the debate on privacy issues at both the state and federal level.

Security Breaches a Top Priority

These laws have also placed a higher focus on certain business activities, with security breaches and identity theft at the top of the list. The California activities are ''upping the ante'' for companies that face security breaches or other losses of information that may result in identity theft. The ''best practices'' in California for security of consumer information are quite broad—and touch on the following topics:

- Collection of the minimum amount of personal information necessary and retention for the minimum time necessary (potentially broadening the Health Insurance Portability and Accountability Act (HIPAA) ''minimum necessary'' concept in two directions—both as to collection of information and reaching entities outside the health care industry)
- Classification of personal information according to sensitivity (a concept in many laws, but not in the broadest laws, such as HIPAA and GLB);
- Use of appropriate physical and technological security safeguards and application to information that is on paper as well as electronic (a concept found in the HIPAA privacy rule, but now extended in California beyond industries regulated at the federal level); and
- Requiring third-party service providers to follow your security policies and procedures—and monitoring and enforcement of these standards (potentially the largest scope of change, as few laws today require active monitoring of vendors). Will this concept catch on at a broader level as the evidence of specific security problems mounts?

So, how will these best practices affect security procedures under both HIPAA and GLB, or other ''best practices'' that should be taken by businesses to protect their customers against identity theft concerns? Regulators and litigants nationwide may seek to use the California best practices as benchmarks far beyond the borders of that state.

What to Make of All This?

With all this complexity, what should companies be doing now?

♦ *Direct Applicability*

Companies in all industries—regardless of where the company is located—must understand their direct compliance obligations under these California laws. Do you have customers in California or otherwise do business in California in a way that permits these laws to touch you? Just because you are based in another state, do not assume that you can escape the reach of these laws. While there may be significant defenses to lawsuits or enforcement actions based on a lack of contacts with California, these laws (for the most part) intend to reach any business that deals with California customers.

♦ *Different Procedures for Different Places?*

To the extent that the California laws do apply to your business, can you ''change'' your procedures only for California? Companies need to understand their business activities in sufficient detail to know whether changes made to comply with California laws can be done only for California residents or businesses, or whether these changes will need to be made on a broader basis. (Obviously, part of this analysis is whether to make the changes in California that would need to carry over across the country).

♦ *Following Where Else These Issues Develop*

Beyond this initial feasibility choice, companies should evaluate whether California is ''going at this alone,'' or whether the California actions will have a broader effect. Does this in turn suggest changing your practices on a broader level—even if it's only for California today? For example, on the Social Security number legislation, a company that changed its practices only for California residents will now find that it is out of compliance with laws in many other states, and that the national trend is clearly towards more restricted use of SSNs. Therefore, understanding the traction of these issues across the country is essential.

♦ *Developing an Appropriate Compliance Program*

Once you have evaluated these various components, and determined how your company views the ''risk management'' components of a California privacy compliance effort, the next key step is to determine how you plan to bring your operations into compliance with the California laws. This will involve a combination of steps—including assessing whether your current practices violate California requirements, how to change the practices to comply, and how broadly to implement these changes. It will be critical to ensure that this compliance program also includes an ongoing program to monitor changes in the law, so that the operational program can stay in line with this rapidly changing legal area. Developing an appropriate compliance program—and factoring in the overall trends in privacy and security regulation—will be the most significant challenge for any company that uses or discloses personal information.

Conclusion

So, while California is moving quickly, and it is fair to say that there is real doubt as to whether this privacy ''scattershot'' approach makes any sense or has any real effects on protecting the private information of consumers, all businesses that deal with customer information need to be aware of these California statutes, and be evaluating how to stay on top of relevant privacy developments across the country.

Beyond this ''awareness'' component, California has demonstrated the lasting interest in privacy as a regulatory issue. The debate in California has been

PVLR ISSN 1538-3423

spirited and durable. Despite substantial lobbying contributions and efforts by a wide range of industries, politicians in California found that their voting support for enhanced privacy regulation outweighed the usual successful lobbying efforts. Will privacy and security be a more visible political issue around the country? Obviously, while national security issues have affected the overall privacy debate in certain settings, the most lasting result of the California experience in 2003 may be to reinvigorate privacy in the commercial arena as a subject that will generate new debate and new regulations. Companies across the country should be developing their business plans and compliance strategies with this revived debate in mind.