International Lawyer

Volume 42
Number 2 *International Legal Developments in Review: 2007*

Article 23

2008

Information Services, Technology and Data Protection Committee

Nicole Beliveau

Lindsay Bleiter

Jacqueline Klosek

Nidhi Kumar

Young Lee

See next page for additional authors

Information Services, Technology and Data Protection Committee

Authors

Nicole Beliveau, Lindsay Bleiter, Jacqueline Klosek, Nidhi Kumar, Young Lee, and James Shreve

Information Services, Technology and Data Protection Committee

COMMITTEE EDITOR: JACQUELINE KLOSEK, GOODWIN—PROCTER LLP

CONTRIBUTING AUTHORS: NICOLE BELIVEAU, LINDSAY BLEIER, JACQUELINE KLOSEK, NIDHI KUMAR, YOUNG LEE, AND JAMES SHREVE

I. Introduction

A. OVERVIEW

As various technologies, businesses, and criminal elements continue to become more advanced and sophisticated, legislators, regulators, and consumer protection authorities continue to struggle to keep pace. In our year-in-review, we present a summary of some of the most significant developments that have occurred over the past year. We commence with a summary of recent trends and then highlight key developments at the federal and state levels within the United States.

B. TRENDS AND POLICY DEVELOPMENTS

1. *Data Security Breaches*

During the past year, dozens of reported high-profile breaches in data security continued. As reports of data security problems and identity theft continue to increase, companies' data security policies will be subject to increased scrutiny. Thus, businesses must ensure that they have appropriate security policies in place to protect their customers' personal data.

Although a number of data security incidents occurred in 2007, two are most noteworthy: (1) the TJX data theft and (2) the loss by the British government of citizens' data.

The TJX incident affected, at last estimate, over 40 million accounts[1] and has spawned a number of lawsuits against both the retailer, TJX,[2] and Fifth Third Bank,[3] its card processor. As mentioned above, another result of the TJX incident is a push by credit card issuing banks to pass along the costs of card reissuance to merchants experiencing a security breach.

In November 2007, the British government announced that two computer disks containing the personal information of 25 million citizens had been lost.[4] In the immediate aftermath of the incident, some in the United Kingdom and throughout Europe began to consider whether a security breach notice requirement along the lines of those enacted in the United States might provide useful protections for consumers.[5]

As discussed below, the continued data insecurity instances have triggered proposals for state and federal legislation addressing data privacy and security, including requiring entities to notify individuals in the event a breach in data security compromises their personal data.

2. *Behavioral Advertising and Online Regulation*[6]

During 2007, there was significant consolidation in the online advertising marketplace. Among the most significant acquisitions were Google-DoubleClick, Yahoo-Right Media, AOL- TACODA, and Microsoft-aQuantive. These transactions signal that the advertising field is transforming at a dramatic pace as key players are combining forces to remain competitive. Accompanying this tremendous change is concern for consumers' privacy.

Of all the recent acquisitions, the Google-DoubleClick deal appears to be the most controversial. Presently, the deal is under scrutiny by the Federal Trade Commission (FTC) and the European Commission.[7] In September, the U.S. Senate Committee on the Judiciary held a hearing to examine the merger.[8] The primary concern regarding the deal is the potential concentration of user data in one company's control. Google maintains a large database of users' search history and Internet preferences, while DoubleClick is a leader in aggregating information on Internet preferences. Google's extensive library of user information coupled with DoubleClick's business model of consumer profiling

1. *See* Jenn Abelson, *Breach of Data at TJX is Called the Biggest Ever: Stolen Numbers Put at 45.7 Million*, BOSTON GLOBE, Mar. 29, 2007, at A1.

2. *See, e.g., Banks Sue TJX over Breach*, WALL ST. J., Apr 26, 2007, at B4.

3. Mel Duvall, *TJX Breach Update: 94 Million Credit Accounts Potentially Exposed*, BASELINE.COM, Oct. 24 2007, http://www.baselinemag.com/c/a/Projects-Security/TJX-Breach-Update-94-Million-Credit-Accounts-Potentially-Exposed/.

4. Cassel Bryan-Low, *Britain's Data Breach Has Banks Alert for Signs of Fraud*, WALL ST. J., Nov. 23, 2007, at A7.

5. *Id.*

6. This section was authored by Nidhi Kumar, an associate with Goodwin Procter, LLP, located at 599 Lexington Avenue, New York, NY 10022. She may be reached at nkumar@goodwinporcter.com or (212) 813-8883.

7. Dawn Kawamoto & Elinor Mills, *Google-DoubleClick: Tough Sell in E.U.*, CNET NEWS.COM, Nov. 21, 2007, http://www.news.com/Google-DoubleClick-Tough-sell-in-EU/2100-1030_3-6219589.html.

8. *An Examination of the Google-DoubleClick Merger and the Online Advertising Industry: What Are the Risks for Competition and Privacy: Hearing Before the Subcomm. on Antitrust, Competition Policy, and Consumer Rights of the S. Comm. on the Judiciary*, 110th Cong. 110-25 (2007), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_senate_hearings&docid=f:39015.pdf.

could enable them to build extremely intimate portraits of individuals and unfairly exploit such information.[9] The FTC is in a unique position in that it has the authority to review this deal from the privacy angle as well as the traditional antitrust angle.

Interestingly, there is no legislation governing online advertising practices. In 2000, the Network Advertising Initiative (NAI), a small coalition of companies in the Internet advertising industry, published self-regulatory principles as a result of several meetings among the NAI, the FTC, and the Department of Commerce[10]; however, public interest groups such as the Electronic Privacy Information Center have claimed that these principles are ineffective.[11] Meanwhile, federal and state lawmakers may be hesitant to pass formal legislation for fear that it may stifle innovation and limit consumers' free access to information over the Internet.

In response to the recent exponential growth of online advertising, the FTC hosted a two-day "town hall" meeting at the beginning of November 2007 where consumer advocates, industry representatives, technology experts, and academics convened to discuss online advertising practices, with a specific focus on consumer protection issues arising out of behavioral advertising or the practice of tracking Internet users' activities online.[12] For the first time since 2000, the FTC considered the privacy implications of new advertising technologies on an industry-wide level.

During the meeting, industry representatives emphasized that targeted online advertising benefits consumers by showing them ads that are useful, relevant, and pertinent to their particular interests while consumer advocates argued that sophisticated targeting technologies endanger consumers' fundamental rights of privacy and are deceptive because consumers are not fully aware of what data is collected and how it is used.[13] In their defense, industry representatives explained that companies such as Google, Microsoft, and Yahoo! are implementing protective measures such as anonymizing user information, limiting data retention to finite periods, reducing cookie lifespan, and disclosing more information to users on how data is stored and used.[14]

Several recommendations for regulating the industry were posed during the meeting, including a "Do Not Track List" inspired by the Do-Not-Call legislation[15] for telephone solicitations, and use of an opt-in versus opt-out feature that would offer consumers more control over their personal information. Another proposal was to require online publishers and advertisers to post more clear and comprehensible disclosures regarding their pri-

9. Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief, In the Matter of Google, Inc. and DoubleClick, Inc., FTC File No. 071 0170 (June 6, 2007), *available at* http://epic.org/privacy/ftc/google/supp_060607.pdf.

10. *See* FTC, ONLINE PROFILING: A REPORT TO CONGRESS (2000), *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf; FTC, ONLINE PROFILING: A REPORT TO CONGRESS, PART 2 RECOMMENDATIONS (2000), *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.htm.

11. *See* ELEC. PRIVACY INFO. CTR., Network Advertising Initiative: Principles Not Privacy, (July 2000), *available at* http://www.epic.org/privacy/internet/NAI_analysis.html.

12. The complete web-cast of the FTC's town hall meeting is available at http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/FTCindex.html#Nov1_07. A transcript has not yet been made available.

13. *Id.*

14. *Id.*

15. Do-Not-Call Implementation Act, 15 U.S.C. § 6101.

vacy policies.[16] It was also recommended that the FTC adopt a new definition for personally identifiable information "as anything that permits 'a set of behaviors or actions to be consistently associated with a particular individual or computer user, even if the individual or computer user is never identified by name or other individual identifier.'"[17]

Despite the significant concerns voiced on behalf of consumers in connection with increasingly sophisticated advertising online, social networking sites such as Facebook and MySpace appear unaffected. Within a few days after the town hall meeting, both these sites announced new ad campaigns that trigger the same privacy issues that the town hall was meant to address and of which the industry was supposed to have been warned.[18]

C. Federal Legislative Developments

1. *Pretexting Rules*[19]

Pretexting involves obtaining certain forms of non-public personal data under false pretenses. Federal law regulates pretexting involving the obtaining of financial information via intentional deceit (including fraudulent statements and impersonation) as part of the Gramm-Leach-Bliley Act (the "GLB Act")[20]. Under the GLB Act, it is also illegal to knowingly solicit others to engage in pretexting.[21]

Within the last year, legislators have begun to pay specific attention to the use of pretexting to obtain personal phone records. Currently, at least fifteen states have enacted laws to regulate the disclosure of phone records. Generally, these state laws prohibit purchasing or selling telephone records obtained without the consent of the subscriber or obtained through the use of fraud or deceit. But the scope of the law varies from state to state.[22] The penalties imposed for violating these state laws vary, with some states providing for felony convictions for violations.[23] Additionally, some states allow customers to bring a private right of action.[24]

The Hewlett-Packard scandal in 2006 prompted new legislation at the federal level dealing specifically with the use of pretexting to obtain personal phone records. In that scandal, Hewlett-Packard hired investigators who used false pretenses to obtain phone records of journalists and Hewlett-Packard board members in an attempt to find out the

16. FTC, Ehavioral Advertising: Tracking, Targeting, and Technology, *available at* http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml.

17. Kate Kaye, *FTC Forum Promises Discussion of More than Just Behavioral*, ClickZ Network, Nov. 1, 2007, http://www.clickz.com/3627473.

18. *See* Anne Schleicher, *Facebook, MySpace Launch New Targeted Ads*, NewsHour Extra, Nov. 7, 2007, *available at* http://www.pbs.org/newshour/extra/features/july-dec07/social_11-07.html; Wendy Davis, *New Facebook, MySpace Ad Programs Prompt FTC Complaint*, Online Media Daily, Nov. 12, 2007, http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticleHomePage&art_aid=70793.

19. This section was authored by Nicole Beliveau, an associate with Goodwin Procter, LLP, located at 599 Lexington Avenue, New York, NY 10022. She may be reached at nbeliveau@goodwinprocter.com or (212) 813-8825.

20. Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6821-6827.

21. *Id.* § 6821(b).

22. *See* Michael Hintze, *Making Sense of Privacy and Security Laws and Regulations: Selected Developments over the Last 12 Months*, 902 PLI/Pat 71, 94-95 (2007).

23. *Id.*

24. *Id.*

source of certain leaks of company information.[25] On January 12, 2007, President Bush signed into law the Telephone Records and Privacy Protection Act of 2006 (the "TRPP Act") to address situations just like that in Hewlett-Packard.[26]

The TRPP Act makes it a crime to: (a) knowingly and intentionally obtain any confidential phone records information by fraudulent means;[27] (b) knowingly and intentionally sell or transfer, or attempt to sell or transfer, confidential phone records information without the prior authorization of the customer (except in certain limited circumstances permitted by other applicable laws);[28] and (c) knowingly and intentionally purchase or receive, or attempt to purchase or receive, confidential records obtained by the methods set forth in subsections (a) and (b).[29]

Violations of the TRPP Act are punishable by fines and/or up to ten years imprisonment.[30] Additional penalties may be imposed for certain more serious violations: (a) violations committed in connection with other criminal behavior and involving more than $100,000 or more than fifty customers occurring in a twelve-month period may be punishable by doubled fines and/or up to five additional years of imprisonment; and (b) violations involving use of confidential phone records information to commit crimes of violence, crimes of domestic violence, or crimes against law enforcement officials are punishable by up to five additional years of imprisonment.[31]

The TRPP Act applies not only to traditional telephone services but also to any Internet-protocol-enabled voice service if the "service can originate traffic to, or terminate traffic from, the public switched telephone network, or a successor network."[32]

2. *CPNI Rules*[33]

The Federal Communications Commission (FCC) issued an order to address the growing concerns over privacy and protection of Customer Proprietary Network Information (CPNI).[34] By imposing stricter access, authentication, disclosure, compliance, and enforcement standards while simultaneously expanding the scope of the CPNI rules, the FCC aims to prevent unauthorized disclosures of CPNI.[35]

---

25. On the Hewlett-Packard case in particular, *see, e.g.*, Complaint, California v. Hewlett-Packard Co., No. 106 CV-076081 (Cal. Super. Ct., Dec. 7, 2006), *available at* http://ag.ca.gov/hpsettlement/pdf/hp_Complaint.pdf; Final Judgment & Permanent Injunction, California v. Hewlett-Packard Co., No. 106 CV-076081 (Cal. Super. Ct., Dec. 7, 2006), *available at* http://ag.ca.gov/cms_attachments/press/pdfs/2007-07-26_hp_Judgment.pdf.

26. 18 U.S.C. § 1039 (2007).

27. *Id.* § 1039 (a).

28. *Id.* § 1039 (b).

29. *Id.* § 1039 (c).

30. *Id.* § 1039 (a)-(c).

31. *Id.* § 1039 (d)-(e).

32. *Id.* § 1039 (h)(4).

33. This section was authored by Young Lee, an associate with Goodwin Procter, LLP, located at 599 Lexington Avenue, New York, NY 10022. He may be reached at ylee@goodwinprocter.com or (212) 813-8821.

34. *In re* Implementation of the Telecomm. Act of 1996: Telecomm. Carriers' Use of Customer Proprietary Network Information & Other Customer Info, 22 F.C.C.R. 6927 (2007) (report & order & further notice of proposed rulemaking).

35. *See id.* ¶¶ 5-9.

Under the order, "providers of interconnected VoIP service" ("Providers") are now subject to the FCC's CPNI rules.[36] The FCC justified this expansion in the scope of the CPNI rules by relying on its ancillary jurisdiction under Title I of the Communications Act.[37]

Under the new CPNI rules, telecommunication carriers ("Carriers") and Providers are subject to new authentication requirements. First, they are prohibited from releasing call detail information[38] during a customer-initiated telephone contact unless: (i) the customer provides the correct pre-established password; (ii) the Carrier or Provider sends the call detail information to the customer's address of record upon the customer's request; or (iii) the Carrier or Provider calls the customer's telephone number of record to disclose the call detail information.[39] Second, all Carriers and Providers must now provide mandatory password protection for online account access to all CPNI. Third, if a customer requests access to CPNI at a Carrier's retail location, a valid photo ID that matches the name on the account must be provided.[40]

The new CPNI rules require Carriers and Providers to provide notification to a customer of the creation or alteration of the customer's: (i) password; (ii) response to back-up means of authentication for lost or forgotten passwords; (iii) online account; or (iv) address of record.[41] The Carrier or Provider may make such notification by voicemail, text message, or mail, each to the customer's information of record on the account.[42] If an unauthorized disclosure of CPNI occurs, the Carrier or Provider must notify federal law enforcement within seven business days via an electronic report.[43] Customer notification must follow within seven business days of the notification to law enforcement unless there is an applicable exception.[44]

In a significant paradigm shift, the order now requires Carriers and Providers to obtain an express, opt-in consent from a customer before any CPNI can be disclosed to a joint venture partner or independent contractor for marketing communications-related services.[45] Under the previous rules, a Carrier would be free to share CPNI with a third party unless a customer expressly opted out after a notification of the Carrier's intent to disclose CPNI to third parties for marketing purposes.[46] The FCC states that the new rules are in direct response to the exponential growth in the black market for CPNI, coupled with concrete evidence that the dissemination of CPNI inflicts specific and significant harm to customers.[47]

---

36. *Id.* ¶ 3.

37. *Id.* ¶¶ 54-55.

38. The FCC considers any information that pertains to the transmission of specific telephone calls as call detail information. An example of a non-call detail CPNI provided by the FCC includes remaining minutes of use. *Id.* ¶ 13 n.45; Carriers and Providers may disclose non-call detail CPNI to a customer upon authentication. *Id.* ¶ 13.

39. *Id.* ¶ 3.

40. *Id.* ¶ 15 n.57.

41. *Id.* ¶¶ 3, 24.

42. *Id.* ¶ 24.

43. Federal law enforcement is the U.S. Secret Service and Federal Bureau of Investigation. *Id.* ¶ 29.

44. In certain circumstances of irreparable harm, customer notification can occur immediately. *Id.* ¶ 29.

45. *Id.* at ¶¶ 37-50.

46. *Id.*

47. *Id.*

Under the previous rules, Carriers were already required to file an annual CPNI compliance certificate, authored by an officer of the company, stating that the company has established operating procedures that are adequate to protect CPNI.[48] The new CPNI rules now require that a more comprehensive annual compliance certificate be filed by all Carriers and Providers, which includes an explanation of any actions taken against data brokers as well as a summary of all consumer complaints received in the past year regarding the unauthorized release of CPNI.[49]

Under the new CPNI rules, Carriers and Providers are required to take reasonable measures to protect CPNI from unauthorized disclosures.[50] Sanctions may be issued to any Carrier or Provider that fails to protect CPNI.[51] In any FCC investigation, Carriers and Providers are on notice that the FCC will infer from evidence of an unauthorized disclosure of CPNI that the Carrier or Provider has failed to take reasonable precautions to protect CPNI.[52] It should also be noted that the FCC declined to provide Carriers and Providers with a Safe Harbor provision under the new CPNI rules.[53]

3. *Data Security Breach*

a. Reglatory Developments

In March 2007, the federal banking regulatory agencies, the FTC, and the Securities and Exchange Commission (SEC) issued model privacy notices to be used by regulated businesses in meeting notice requirements under the GLB Act.[54] The model notices were issued as a proposed rule, and public comments were sought by the regulators.

In October 2007, the federal banking regulatory agencies and the FTC issued a final rule outlining steps to avoid identity theft.[55] The so-called Red Flags Rule requires a financial institution to develop and implement an identity theft prevention program commensurate to its size and the risks it faces. The Red Flags Rule also lists a number of specific actions that may be indicative of an identity theft attempt and that should prompt increased scrutiny by financial institutions. Compliance with the Red Flags Rule is mandatory by November 1, 2008.

In October 2007, the federal banking regulatory agencies issued final rules governing certain information sharing arrangements for marketing purposes by financial institutions.[56] The Affiliate Marketing Rule will require consumer notice and an opportunity for opt-out by the consumer before a consumer's transaction or account relationship information (information from applications submitted by the consumer or third party sourced information such as credit reports) is shared among affiliated entities to market products

48. *Id.* ¶ 52.
49. *Id.* ¶ 51.
50. *Id.* ¶ 63.
51. *Id.*
52. *Id.*
53. *Id.* ¶ 66.
54. Interagency Proposal for Model Privacy Form Under the Gramm-Leach-Bliley Act, 72 Fed. Reg. 16,875 (Apr. 5, 2007).
55. Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63,718 (Nov. 9, 2007).
56. Fair Credit Reporting Affiliate Marketing Regulations, 72 Fed. Reg. 62,910 (Nov. 7, 2007).

or services to the consumer. Compliance with the Affiliate Marketing Rule is mandatory by October 1, 2008.

D. SIGNIFICANT STATE DEVELOPMENTS

1. *Radio Frequency Identification Devices*[57]

Several legislative initiatives regarding radio frequency identification devices (RFID) were proposed in 2007, but only a few notable bills were passed at the state level. Reacting to concern over the possibility of human RFID implantation, North Dakota enacted a new section of its criminal code in April prohibiting any person from requiring "that an individual have inserted into that individual's body a microchip containing a radio frequency identification device."[58] Border states like Texas[59] and Washington[60] also enacted legislation in response to increasing concerns over the security of U.S. borders and the efficiency related to legal border crossings. Ever since Wal-Mart announced in 2004 its proposal to tag goods carried in its stores with RFID,[61] legislators considering RFID have focused predominantly on privacy concerns and seemed to overlook any related benefits. This stems in part from the fact many lawmakers fail to appreciate RFID's benefits as well as their already prevalent use in many consumer goods, including cell phones, contact-free credit cards, and toll road transmitters like E-Z Pass.

---

57. This section was authored by Lindsay Bleirer, an associate with Goodwin Procter, LLP, located at 599 Lexington Avenue, New York, NY 10022. She may be reached at lbleier@goodwinprocter.com or (212) 459-7209.

58. N.D. CENT. CODE. § 12.1-15-06 (2007).

59. In an act "relating to homeland security and protection of the public, including protections against human trafficking," the Texas legislature enacted a bill in June requiring that

> enhanced driver's license[s] or personal identification certificate[s] must include reasonable security measures to protect the privacy of the license or certificate holders, including reasonable safeguards to protect against the unauthorized disclosure of information about the holders. If the enhanced driver's license or identification certificate includes a radio frequency identification chip or similar technology, the department shall ensure that the technology is encrypted or otherwise secure from unauthorized information access.

2007 TEX. SESS. LAW. SERV. ch. 258 (West).

In that same Act, Texas prohibited anyone from selling or otherwise disclosing "biometric information accessed from an enhanced driver's license or any information from an enhanced driver's license radio frequency identification chip or similar technology to another person or an affiliate of the person." *Id.*

60. In March, Washington enacted legislation requiring that its

> enhanced driver's license or identicard must include reasonable security measures to protect the privacy of Washington state residents, including reasonable safeguards to protect against unauthorized disclosure of data about Washington state residents. If the enhanced driver's license or identicard includes a radio frequency identification chip, or similar technology, the department shall ensure that the technology is encrypted or otherwise secure from unauthorized data access.

WASH. REV. CODE. ANN. § 46.20.202 (West 2008).

61. *See, e.g.*, InformationWeek, *Wal-Mart's RFID Plans to Be Put to the Test*, Mar. 29, 2004, http://www.informationweek.com/story/showArticle.jhtml?articleID=18402888.

2. *Spyware*[62]

The regulation of spyware continues to be a major issue for many state lawmakers. In 2007, legislation concerning spyware was introduced in at least fourteen states and enacted in Arkansas and Virginia. Arkansas established a Spyware Monitoring Fund to offset expenses directly related to the enforcement of the Consumer Protection Against Computer Spyware Act.[63] Virginia now makes it a felony for a person to "install or cause to be installed, or collect information through" software capable of recording keystrokes "on the computer of another."[64]

3. *Data Security Breaches*

By May 2008, forty-three states had enacted laws requiring notice be provided to affected state residents in the event of a security breach. The breach notice laws in Hawaii, New Hampshire, Utah, Vermont, the District of Columbia, Wyoming, Michigan, Oregon, and Massachusetts became effective in 2007, and the Maryland breach notice law became effective in January 2008.[65] Newly enacted laws in Virginia and West Virginia will become effective in mid-2008 and a South Carolina law takes effect in 2009.[66]

Some states that had enacted security breach notice requirements in previous years began revising, and often expanding, the coverage of the requirements in 2007. One noteworthy trend in security breach notice legislation is the introduction of provisions permitting credit card issuing banks to recoup some of the costs incurred from a security breach from merchants not following data security standards. Massachusetts first considered such a provision in the wake of the TJX incident.[67] Although that provision did not survive in the enacted Massachusetts law, Minnesota did pass a similar cost recoupment provision.[68] The California Assembly passed a bill containing a similar provision,[69] but the bill was vetoed by Governor Schwarzenegger.[70] Reports indicate that California is again considering such legislation and similar bills are pending in other states.[71]

---

62. This section was authored by Lindsay Bleirer, an associate with Goodwin Procter, LLP, located at 599 Lexington Avenue, New York, NY 10022; She may be reached at lbleier@goodwinprocter.com or (212) 459-7209.

63. 2005 Ark. Acts 2255; *see also* ARK. CODE ANN. § 19-6-804 (West 2007).

64. VA. CODE ANN. § 18.2-152.4 (West 2008).

65. HAW. REV. STAT. § 487N-1 *et seq.* (2007); N.H. REV. STAT. ANN. § 359-C:19 *et seq.* (2008); UTAH CODE ANN. § 13-44-101 *et seq.* (West 2007); VT. STAT. ANN. tit. 9, § 2430 *et seq.* (2008); D.C. CODE § 28-3851 *et seq.* (2008); WYO. STAT. ANN. § 40-12-501 *et seq.* (2007); MICH. COMP. LAWS ANN. § 445.61 *et seq.* (West 2008); OR. S.B. 583, 74th Gen. Assem., Reg Sess. (Or. 2007); MASS. GEN LAWS ANN. ch. 93H, § 1 *et seq.* (West 2007); MD. CODE ANN., [COM LAW] § 14-3501 *et seq.* (West 2008) (2007).

66. Va. S.B. 307, 2008 Legis. Sess., Reg. Sess. (Va. 2008); W.Va. S.B. 340, 78th Leg., 2nd Sess. (W.Va. 2008); S.C. S.B. 453, 117th Gen. Assem., 2nd Sess. (S.C. 2008).

67. *See* MASS. GEN. LAWS ANN. ch. 66B, § 1 *et seq.* (West 2008).

68. The cost reimbursement provision becomes effective on August 1, 2008. MINN. STAT. § 325E. 64 (2008).

69. *See* Assemb. B. 779, 2007 Leg. (Cal. 2007), *available at* http://info.sen.ca.gov/pub/07-08/bill/asm/ab_0751-0800/ab_779_bill_20070914_enrolled.pdf.

70. *See* Letter from Governor Arnold Schwarzenegger to Members of the California State Assembly (Oct. 13, 2007), *available at* http://info.sen.ca.gov/pub/07-08/bill/asm/ab_0751-0800/ab_779_vt_20071013.html.

71. *See* Laura Mahoney, *Bill to Broaden California's Breach Notification Law Passes Assembly*, PRIVACY LAW WATCH, Apr. 24, 2008; Ala. S.B. 489 & S.B. 544, 2008 Legis. Sess., Reg. Sess. (Ala. 2008); Mich. S.B. 1022, 94th Leg., Reg. Sess. (Mich. 2008); N.J. A. 2270, 2008-2009 Legis. Sess. (N.J. 2008).

II. Conclusion

Many observers have speculated that, with the recent political shift in Congress and the upcoming presidential elections, we will see enhanced legislative focus on prior issues in the coming years. As companies, organizations, and even governmental agencies continue to be plagued by security breaches—and consumers continue to demand recourse—we are likely to see continued legislative focus on this particular area.