

2010 Privacy and Data Security Developments

By Patricia E.M. Covington and Meghan Musselman*

INTRODUCTION

The year 2010 marked the end of a decade in which privacy and data security proved to be one of the most cutting-edge and constantly evolving areas of law. Legislatures and regulatory agencies at both the federal and state level worked to keep pace with technological advances and the need for consumer protection. The decade began with the enactment of the Gramm-Leach-Bliley Act (“GLB Act”)¹ in November 1999, signifying the first time financial institutions were required to give consumers a notice detailing how personal information about them is collected and shared. The GLB Act also introduced the concept of safeguarding consumer information to non-bank financial institutions.² Safeguarding gained importance when California enacted its security breach notice law in 2003.³ Almost every state followed California’s lead and enacted its own security breach notice law.⁴ Some states went further and enacted a host of other privacy and data security laws.⁵

Meanwhile regulators, particularly the Federal Trade Commission (“FTC”), vigilantly and zealously enforced new and existing laws against companies that

* Patricia E.M. Covington is a partner in the Maryland Office of Hudson Cook, LLP. She is Chair of the Privacy Subcommittee of the Committee on Consumer Financial Services of the American Bar Association Section of Business Law and is the Liaison from the Committee on Consumer Financial Services to the American Bar Association Anti-Money Laundering Task Force. Meghan Musselman is a partner in the Maryland office of Hudson Cook, LLP. She is Vice Chair of the Legislation and Regulation Subcommittee of the Banking Law Committee of the Section of Business Law and a member of the Executive Council of the Federal Bar Association’s Banking Law Committee.

1. Pub. L. No. 106-102, tit. V, 113 Stat. 1338, 1436 (1999) (codified as amended at 15 U.S.C. §§ 6801–6809 (2006)).

2. See 15 U.S.C. § 6801(b); see also Federal Trade Commission, Safeguards Rule, 16 C.F.R. pt. 314 (2010); Regulation P, 12 C.F.R. pt. 216 (2010).

3. See CAL. FIN. CODE §§ 4050–4060 (West Supp. 2009).

4. Patricia E.M. Covington & Meghan Musselman, *Privacy and Data Security Developments Affecting Consumer Finance in 2008*, 64 BUS. LAW. 533, 535–36 (2009) (in the 2009 Annual Survey) (“Virtually every state’s security breach notice law contains some form of the [notice] provisions noted above. These provisions are derived from California’s security breach notice law, which was the first of its kind. . . . Forty-four states now have some form of security breach notice law.” (footnote omitted)).

5. See Patricia E.M. Covington & Meghan Musselman, *Recent Privacy and Data Security Developments*, 65 BUS. LAW. 611, 618–19 (2010) (in the 2010 Annual Survey) (“The newest trend in state privacy legislation and regulation is the imposition of detailed safeguarding requirements.”); see also Covington & Musselman, *supra* note 4, at 541–43.

either failed to safeguard consumer information adequately or did not keep their promises about how consumer information was maintained, used, or shared.⁶ The decade ended on a slower pace, albeit with continued zealous enforcement of privacy and security laws and a pioneering law holding retailers liable for security breaches.⁷ The current climate is one of study and reflection regarding what course privacy and data security law should take in the coming decade, particularly as it relates to online and mobile technologies.⁸ There are hints of what is to come in proposed legislation and statements by FTC commissioners, clearly indicating that privacy, data security, and online activities are priorities.⁹

ONLINE AND BEHAVIORAL MARKETING

THE IMPORTANCE OF ONLINE MARKETING

Online and behavioral marketing is arguably the most rapidly developing area affecting privacy and data security. With the emergence of smartphones, social networking, and wireless internet, consumers spend increasingly more time online, changing how they behave and interact with the world.¹⁰ Consumers maintain contact with friends and family through Facebook and Twitter, have constant access to the web on their smartphones, and rely on Global Positioning Systems (“GPS”) to navigate the physical world. Online shopping is a “given,” and online banking, including loan applications and online bill payment, is prevalent.¹¹ Using mortgage lending as an example, *National Mortgage News* reports that online

6. For a detailed discussion of the actions taken, see Covington & Musselman, *supra* note 5, at 613–15.

7. See Complaint, *In re* Twitter, Inc., No. 092 3093 (FTC filed Jan. 22, 2010), available at <http://www.ftc.gov/os/caselist/0923093/100624twittercmpt.pdf> [hereinafter Twitter Complaint]; 2010 Wash. Legis. Serv. ch. 151 (HB 1149) (West) (to be codified at WASH. REV. CODE § 19.255).

8. See Jon Leibowitz, Chairman, Fed. Trade Comm’n—Prepared Statement of the Federal Trade Commission on Consumer Privacy Before the Committee on Commerce, Science, and Transportation, United States Senate 2 (July 27, 2010), available at <http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf> [hereinafter Prepared Statement] (“The FTC has a long track record of protecting consumer privacy. The Commission’s early work on privacy issues dates back to its initial implementation in 1970 of the Fair Credit Reporting Act . . . which includes provisions to promote the accuracy of credit reporting information and protect the privacy of that information. With the emergence of the Internet and the growth of electronic commerce . . . the FTC expanded its focus to include online privacy issues. Since then, both online and offline privacy issues have been at the forefront of the Commission’s agenda . . .”).

9. See, e.g., David Vladeck, Dir., FTC Bureau of Consumer Prot.—Remarks to the International Association of Privacy Professionals: The Role of the FTC in Consumer Privacy Protection 3 (Dec. 8, 2009), available at <http://www.ftc.gov/speeches/vladeck/091208iapp.pdf>. (“We remain committed to addressing . . . consumer privacy harms, even as we reexamine existing privacy frameworks and identify new areas of concern to consumers.”).

10. See *Led by Facebook, Twitter, Global Time Spent on Social Media Sites Up 82% Year Over Year*, NIELSEN WIRE (Jan. 22, 2010), <http://blog.nielsen.com/nielsenwire/global/led-by-facebook-twitter-global-time-spent-on-social-media-sites-up-82-year-over-year/> (“[G]lobal consumers spent more than five and half [sic] hours on social networking sites like Facebook and Twitter in December 2009, an 82% increase from the same time last year . . .”).

11. See FISERV, 2010 BILLING HOUSEHOLD SURVEY: CONSUMER SURVEY OF OFFLINE AND ONLINE BILLING AND PAYMENT PRACTICES 1 (2010), available at [http://www.fiserv.com/RP_fiserv-2010-billing-household-survey\(1\).pdf](http://www.fiserv.com/RP_fiserv-2010-billing-household-survey(1).pdf) (“As online penetration levels top 75% of all U.S. households, with 65% having

lending activities increased significantly from 2008 to 2009.¹² Loan production increased by 24 percent, the top ten loan providers increased online originations by 22 percent, and online retailers experienced a 90 percent increase in loan production.¹³ Much of this growth is attributed to advances in mobile technology.¹⁴ Consumer-centric businesses, including providers of financial products and services, want to capitalize fully on new technologies and consumers' desire for 24/7 (twenty-four hours a day, seven days a week) connectivity.¹⁵ This is evident as businesses establish a presence on Facebook and Twitter.¹⁶

One way businesses are trying to capitalize on consumers' online presence and associated new technologies is by tracking consumers' online behaviors.¹⁷ This practice is the foundation of targeted advertisements—ads pairing consumers with products and services in real time based on the consumers' online behaviors.¹⁸ Many consumers are unaware that companies are logging their online activities and using them for marketing purposes; this disconnect raises privacy concerns and is a primary reason that Congress and the FTC have made behavioral advertising a priority.¹⁹

broadband connectivity, Americans continue to grow more comfortable with transacting online—especially when it comes to online payment of recurring bills.”).

12. See Anthony Garritano, *Mobile Technology Use Boosts Online Volume*, NAT'L MORTGAGE NEWS, June 18, 2010, at 1 (“According to survey figures compiled by National Mortgage News, online loan production increased 24% in 2009 from the prior year.”).

13. *Id.* (“[O]nline loan production increased 24% in 2009 from the prior year. Online originations by the top 10 providers increased by 22%, but the biggest gains, by far, were achieved among online retailers which grew loan production by 90% during the same time frame.”).

14. *Id.* (“The surge [in originations], many experts believe, was supported by mobile technology.”).

15. See *id.* (“Mobile devices have long been part of our industry’s corporate culture to optimize executives’ time outside the office” (quoting Tyler Sherman, CEO of Motivity Solutions)).

16. See generally Steve Cocheo, *Billboards, Web, Twitter Spearhead Bank’s Comeback*, AM. BANKING J., Sept. 2009, at 14, 14 (“Community banks venturing into social media remain a minority of the industry, and those using Twitter represent a smaller slice of the pie yet.”); Alain Sherter, *Banking on Twitter and Facebook: Wells Fargo’s Smart Social Networking Strategy*, BNET FIN. FOLLY (Apr. 1, 2010), <http://www.bnet.com/blog/financial-business/banking-on-twitter-and-facebook-wells-fargo-8217s-smart-social-networking-strategy/4555>.

17. See generally Julia Angwin, *The Web’s New Gold Mine: Your Secrets*, WALL ST. J., July 30, 2010, at W1; Natasha Singer, *Shoppers Who Can’t Have Secrets*, N.Y. TIMES, May 1, 2010, at BU5.

18. See Jon Leibowitz, Chairman, Fed. Trade Comm’n, Introductory Remarks at FTC Privacy Roundtable 1 (Dec. 7, 2009), available at <http://www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf> [hereinafter Introductory Remarks] (“Behavioral targeting is one of many ways that companies can use data, to try to tease out which consumers—or IP addresses, or uniquely identified cookies—are more likely to respond to a particular ad.”); see also Emily Steel, *Marketers Watch as Friends Interact Online*, WALL ST. J., Apr. 15, 2010, at B5.

19. See Introductory Remarks, *supra* note 18, at 2 (“[T]here are both benefits to companies and consumers from targeting; such as more relevant advertising, and costs in terms of privacy. . . . Consumers have to grapple with this brave new world of information without analogies in their experience, and without a real understanding of the ways their information is handled or transferred.”); see also David C. Vladeck, Dir., FTC Bureau of Consumer Prot., Remarks to the American Teleservices Association Washington Summit 10 (Apr. 27, 2010), available at <http://www.ftc.gov/speeches/vladeck/100427ataspeech.pdf> [hereinafter Teleservices Remarks] (“Let me now move . . . to a ‘hot’ area . . . consumer privacy and, more specifically, the privacy concerns related to behavioral advertising. Ensuring the privacy of consumers’ personal information has been one of the FTC’s top consumer protection priorities for more than a decade.”).

PRIVACY ROUNDTABLES

At present, online and behavioral marketing practices are largely unregulated, both at the federal and state level.²⁰ However, the FTC has emphatically stated that behavioral privacy is a priority and that it is committed to protecting consumers in this area.²¹ From late 2009 through the spring of 2010, the FTC held a series of Privacy Roundtables that explored new technologies used to collect and use consumer information, and how the resulting business practices, including behavioral marketing, affect consumer privacy.²²

In his opening remarks at the inaugural Privacy Roundtable, FTC Chairman Jon Leibowitz said candidly that the FTC was not sure where it was headed, but would proceed with an open mind.²³ He also said that the notice and choice regime and the subsequent harm-based approach to enforcement have limited utility in the current marketplace.²⁴ In remarks made after the Privacy Roundtables concluded, Chairman Leibowitz explained that behavioral advertising implicates both consumer choice and consumer control—consumers are not aware that their habits are being tracked and then have no control over how that information is used.²⁵ He said the current notice and choice regime no longer works because consumers are not giving “informed” consent. Disclosures, he said, are drafted in legalese and buried in long and complex user agreements.²⁶ Nonetheless, as of this

20. Richard Raysman & Peter Brown, *Tech Watch: Developments in Online Behavioral Advertising*, N.Y. L.J., June 8, 2010, at 5, available at <http://www.law.com/jsp/article.jsp?id=1202461024572> (“There is no comprehensive privacy protection legislation in the United States that addresses the collection, storage, transmission, or use of personal information, but rather a patchwork of laws and regulations that peripherally touch on behavioral advertising.”).

21. See Teleservices Remarks, *supra* note 19, at 10.

22. *Exploring Privacy: A Roundtable Series*, FED. TRADE COMM’N, <http://www.ftc.gov/bcp/workshops/privacyproundtables/index.shtml> (last visited Dec. 26, 2010) (“The Federal Trade Commission will host a series of . . . roundtable discussions to explore the privacy challenges posed by the vast array of 21st century technology and business practices that collect and use consumer data. Such practices include social networking . . . [and] online behavioral advertising The goal of the roundtables is to determine how best to protect consumer privacy while supporting beneficial uses of the information and technological innovation.”).

23. Introductory Remarks, *supra* note 18, at 2–3 (“People have asked me what we expect to get from this roundtable, and where we’re headed. I can honestly say: [W]e don’t know. Our minds are open.”).

24. *Id.* at 3 (“[T]he approaches we’ve tried so far—both the notice and choice regime, and later the harm-based approach—haven’t worked quite as well as we would like.”).

25. Jon Leibowitz, Chairman, Fed. Trade Comm’n—Where’s the Remote? Maintaining Consumer Control in the Age of Behavioral Advertising, Address to the National Cable & Telecommunications Association 2 (May 12, 2010), available at <http://www.ftc.gov/speeches/leibowitz/100512nctaspeech.pdf> [hereinafter *Where’s the Remote*] (“Behavioral advertising raises questions of consumer choice. Consumers often have no idea that advertisers are charting their personal information. . . . Behavioral advertising also raises questions of consumer control. Once advertisers capture personal data, consumers have no say in where or how securely it is stored. And they have little or no recourse if—or when—the data is stolen.”).

26. *See id.* at 3 (“But today, few of us can comprehend the amount of personal data we’ve left open for capture on the Internet, and disclosure forms are most often written by lawyers, paid, it seems, by the syllable.”).

writing, the FTC does not intend to regulate behavioral marketing—at least not in the near term. Chairman Leibowitz expressed “great hopes for self-regulation,” referring to the Self-Regulatory Principles for Online Behavioral Advertising developed by several industry associations.²⁷ “So long as self-regulation is making forward progress,” said Leibowitz, “the FTC is not interested in regulating [behavioral advertising].”²⁸

While the FTC is not currently proposing to regulate behavioral marketing as such, it does intend to suggest ways that privacy can be improved, which could lead to federal legislation and regulation, and encourage stronger self-regulation principles. In testimony before Congress, the FTC identified the following priorities: (i) integrating privacy and data security measures into every business’s procedures, systems, and technologies; (ii) simplifying online privacy choices for consumers; and (iii) improving transparency about how data is used.²⁹

DATA PASS

“Data pass” is a practice related to online marketing that recently surfaced as a hot-button issue. Data pass occurs during the checkout process when a consumer is making an online purchase.³⁰ While checking out, the consumer is offered a discount or reward offer; upon accepting the offer, the customer commits to membership or other recurring fees.³¹ These membership offers come from third parties, not from the merchant from whom the consumer is making the purchase.³² Many consumers do not realize that a third party is involved or that he or she has entered into an additional transaction.³³ The confusion arises because the consumer does not realize that the third party already has the consumer’s credit card information, having obtained it from the merchant.³⁴ The concern is that consumers are committing to these transac-

27. See *id.* (citing AM. ASS’N OF ADVER. AGENCIES, ASS’N OF NAT’L ADVERTISERS, COUNCIL OF BETTER BUS. BUREAUS, DIRECT MKTG. ASS’N & INTERACTIVE ADVER. BUREAU, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009)). Examples of online behavioral advertising include online tracking and data collection. See *Privacy Implications of Online Advertising: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 110th Cong. 2 (2008) (statement of Lydia Parnes, Director, Bureau of Consumer Protection, Federal Trade Commission).

28. Where’s the Remote?, *supra* note 25, at 3.

29. Prepared Statement, *supra* note 8, at 21, 22–25.

30. See Press Release, Visa, Visa Helps Protect Consumers from Deceptive Marketing (Apr. 27, 2010), available at <http://corporate.visa.com/media-center/press-releases/press1011.jsp> [hereinafter Visa Press Release] (“[D]ata pass’ usually involves a consumer shopping at a familiar retailer. At checkout, the consumer receives an offer for a discount or reward and does not realize it is from a different merchant and comes with unexpected monthly membership fees or recurring charges.”).

31. *Id.*

32. *Id.*

33. *Id.*

34. Restore Online Shoppers’ Confidence Act, S. 3386, 111th Cong. § 2(5) (2010) (“These third party ‘post-transaction’ offers were designed to make consumers think the offers were part of the initial purchase, rather than a new transaction with a new seller.”).

tions under false pretenses, expecting that they must re-enter their payment information before they will become obligated on an additional transaction.³⁵ The Commerce Committee of the U.S. Senate reported in 2009 that 35 million consumers have paid \$1.4 billion for marketing offers received through the use of data pass practices.³⁶

There have been two significant developments over the past year relating to data pass. First, Visa announced a voluntary initiative that will prohibit internet merchants from providing cardholder information to third parties without the consumer's knowledge or active consent.³⁷ Visa has historically prohibited merchants from sharing account or transaction information with a third party not involved in the transaction.³⁸ Visa amended its rules to address more directly data pass by requiring retailers to ask consumers affirmatively to re-enter their credit card number before accepting a marketing offer from a third party.³⁹ The intent is to alert consumers that they are committing to an additional transaction that is separate and apart from the original transaction.

The second development was the introduction by Senator John D. Rockefeller IV (D-W. Va.) of legislation to regulate data pass. The Restore Online Shoppers' Confidence Act would prohibit a merchant from providing a consumer's account information to a third-party seller for purposes of a post-transaction sale.⁴⁰ The Act would also require a third-party seller to disclose clearly all material terms of the post-transaction sale, including the fact that the third-party seller is not affiliated with the initial merchant.⁴¹ The third-party seller would also be required to obtain the consumer's express informed consent to charge the consumer's credit card, debit card, or bank account by requiring the consumer to: (i) enter her account number and contact information; and (ii) affirmatively act to demonstrate consent, such as by clicking on a confirmation number or checking a box to in-

35. *Id.* § 2(7) ("The use of a 'data pass' process defied consumers' expectations that they could only be charged for a good or service if they submitted their billing information, including their complete credit or debit card numbers.").

36. OFFICE OF OVERSIGHT & INVESTIGATIONS, MAJORITY STAFF, U.S. SENATE COMM. ON COMMERCE, SCI. & TRANSP., AGGRESSIVE SALES TACTICS ON THE INTERNET AND THEIR IMPACT ON AMERICAN CONSUMERS ii (Nov. 19, 2009), available at <http://commerce.senate.gov/public/index.cfm?p=Reports> ("Affinion, Vertrue, Webloyalty and their e-commerce partners have earned over \$1.4 billion in revenue. . . . Since 1999, Internet consumers have been enrolled more than 35 million times in Affinion, Vertrue, and Webloyalty's membership clubs."); see also OFFICE OF OVERSIGHT & INVESTIGATIONS, MAJORITY STAFF, U.S. SENATE COMM. ON COMMERCE, SCI. & TRANSP. SUPPLEMENTAL REPORT ON AGGRESSIVE SALES TACTICS ON THE INTERNET 1-2 (May 19, 2010), available at <http://commerce.senate.gov/public/index.cfm?p=Reports>.

37. See Visa Press Release, *supra* note 30; see also Press Release, U.S. Senator Jay Rockefeller, Senator Rockefeller Continues to Fight to Protect American Consumers and Combat Aggressive Sales Tactics on the Internet (Dec. 9, 2009), available at <http://rockefeller.senate.gov/press/record.cfm?id=320462>.

38. See Visa Press Release, *supra* note 30.

39. *Id.* ("To address the data-pass practice, merchants will now have to prompt consumers to re-enter their card information to accept a subsequent offer from a third-party merchant. This provides a clear signal to cardholders that a second purchase is being initiated.").

40. Restore Online Shoppers' Confidence Act, S. 3386, 111th Cong. § 3(b) (2010).

41. *Id.* § 3(a)(1) ("[B]efore obtaining the purchaser's billing information, the post-transaction third party seller has clearly and conspicuously disclosed to the purchaser all material terms of the transaction.").

dicating consent to the charge.⁴² The Act left the Senate Committee on Commerce, Science, and Transportation on June 9, 2010.⁴³

PRIVACY NOTICES

Last year's *Annual Survey* reported that the Federal Deposit Insurance Corporation, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the National Credit Union Administration, the FTC, the Commodity Futures Trading Commission, and the U.S. Securities and Exchange Commission (collectively "the Agencies") adopted model privacy notice forms that provide safe harbor protection for the GLB Act privacy notice requirement.⁴⁴ In April 2009, the Agencies released an online form builder that allows financial institutions to create their own privacy notice online.⁴⁵ The online form builder is available in four formats: (i) opt-out and affiliate marketing; (ii) opt-out and no affiliate marketing; (iii) no opt-out and affiliate marketing; and (iv) no opt-out and no affiliate marketing.⁴⁶ Both of the opt-out formats provide for opt-out by telephone or online; they do not allow for a mail-in opt-out option.

DATA SECURITY

FTC ENFORCEMENT ACTIONS

As reported last year,⁴⁷ the FTC has, in recent years, increasingly used its enforcement authority under section 5 of the Federal Trade Commission Act ("FTC Act"),⁴⁸ which prohibits unfair and deceptive acts and practices in the area of data security.⁴⁹ This trend continued in 2010, as the FTC pursued enforcement actions under both the unfair and deceptive prongs of the FTC Act. The first was a landmark settlement with Twitter, Inc. ("Twitter"), a social networking site on which

42. *Id.* § 3(a)(2)(A), (B) ("[T]he post-transaction third party seller has received the express informed consent for the charge from the consumer whose credit card, debit card, bank account, or other financial account will be charged by—(A) obtaining from the consumer—(i) the full account number of the account to be charged; and (ii) the consumer's name and address and a means to contact the consumer; and (B) requiring the consumer to perform an additional affirmative action, such as clicking on a confirmation button or checking a box that indicates the consumer's consent to be charged the amount disclosed.")

43. *See* S. 3386: *Restore Online Shoppers' Confidence Act*, GOVTRACK, <http://www.govtrack.us/congress/bill.xpd?bill=s111-3386> (last visited Dec. 26, 2010).

44. *See* Covington & Musselman, *supra* note 5, at 615 ("On November 17, 2009, the Federal Deposit Insurance Corporation, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the National Credit Union Administration, the Federal Trade Commission, the Commodity Futures Trading Commission, and the U.S. Securities and Exchange Commission . . . adopted final model privacy notice forms pursuant to the GLB Act.")

45. Press Release, Fed. Trade Comm'n, Federal Regulators Release Model Consumer Privacy Notice Online Form Builder (Apr. 15, 2010), available at <http://www.ftc.gov/opa/2010/04/glb.shtm>.

46. *Final Model Privacy Form*, Bd. OF GOVERNORS OF THE FED. RESERVE SYS., http://www.federalreserve.gov/bankinforeg/privacy_notice_instructions.pdf (last visited Dec. 26, 2010).

47. *See* Covington & Musselman, *supra* note 5, at 613.

48. 15 U.S.C. § 45(a)(2) (2006).

49. *Id.*; *see also* Covington & Musselman, *supra* note 5, at 614–15.

users send brief updates called “tweets” to “followers.” “Tweets” are sent in e-mails or text messages, and “followers” are those Twitter users who have requested to receive another user’s tweets.⁵⁰ The Twitter settlement marks the first FTC enforcement action against a social networking service,⁵¹ and demonstrates the FTC’s commitment to staying relevant in the constantly changing technological marketplace. This settlement was based on the deceptive prong of the FTC Act.⁵²

The FTC’s complaint against Twitter stemmed from several incidents in 2009 where individuals gained unauthorized access to the Twitter system.⁵³ Those individuals accessed nonpublic tweets and other nonpublic user information, in addition to resetting user passwords.⁵⁴ A number of the reset passwords were posted on a website and used by others to send unauthorized tweets from the compromised accounts.⁵⁵ Perhaps the most well-known of these was a fraudulent tweet from President Barack Obama’s account offering his followers a chance to win \$500 in free gasoline in exchange for completing a survey.⁵⁶

The FTC alleged that these intrusions occurred as a result of Twitter’s failure to safeguard both its system and the nonpublic information contained in it, which violated its promises to users.⁵⁷ First, the FTC pointed to the privacy policy Twitter posted on its website, which stated: “Twitter is very concerned about safeguarding the confidentiality of your personally identifiable information. We employ administrative, physical, and electronic measures designed to protect your information from unauthorized access.”⁵⁸ The FTC also pointed to other statements made on the Twitter website, particularly those describing privacy controls, for example: “Not everyone has to see your Twitter updates. Keep your Twitter updates private and approve your followers by protecting your profile Protected account owners control who is able to follow them, and keep their updates away from the public eye.”⁵⁹

The FTC charged that Twitter failed to live up to its promises in several respects, mostly because of inadequate policies and procedures concerning administrative passwords and access to information.⁶⁰ Almost all employees had administrative rights to all Twitter user accounts, giving them the ability to: (i) reset a user’s account password; (ii) view a user’s nonpublic tweets and other nonpublic user information; and (iii) send tweets on behalf of a user.⁶¹ To exercise their admin-

50. See Twitter Complaint, *supra* note 7, ¶ 3.

51. Press Release, Fed. Trade Comm’n, Twitter Settles Charges that It Failed to Protect Consumers’ Personal Information (June 24, 2010), available at <http://www.ftc.gov/opa/2010/06/twitter.shtm>.

52. *Id.*

53. Twitter Complaint, *supra* note 7, ¶ 12.

54. *Id.*

55. *Id.*

56. *Id.*

57. *Id.* ¶ 14.

58. *Id.* ¶ 10.

59. *Id.*

60. *Id.* ¶ 11.

61. *Id.* ¶ 7.

istrative rights, Twitter employees used their administrative passwords.⁶² Twitter did not have policies and procedures for using the passwords.⁶³ Specifically, the FTC charged that the passwords were not required to be “hard to guess,” nor were employees required to update their passwords periodically.⁶⁴ In addition, Twitter failed to disable an administrative log-in after a reasonable number of failed attempts.⁶⁵ These shortcomings, the FTC alleged, created vulnerabilities in the Twitter system, allowing intruders to gain easy access through the use of an automated password guessing tool that deciphered an employee’s administrative password.⁶⁶

In a consent order, Twitter agreed to develop and maintain “a comprehensive information security program . . . reasonably designed to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information.”⁶⁷ The consent order sets forth several requirements for the information security program, which largely track the FTC’s Safeguards Rule.⁶⁸ Twitter is also required to have its information security program independently audited every other year for ten years.⁶⁹

The FTC entered into a similar settlement with Dave & Buster’s, Inc. (“Dave & Buster’s”), a restaurant chain that operates throughout the United States and accepts payment by credit and debit card.⁷⁰ However, the FTC based this action on the unfairness prong of the FTC Act.⁷¹ To process debit and credit card payments, Dave & Buster’s collected the credit card number, expiration date, and electronic security code.⁷² An intruder hacked into the Dave & Buster’s computer system, installing unauthorized software and intercepting credit and debit card information for approximately 130,000 customers.⁷³ The FTC alleged that Dave & Buster’s failed to take reasonable steps to protect sensitive personal information collected from customers, and that constituted unfair acts and practices.⁷⁴ The FTC identified the following as system vulnerabilities that led to the breach: (i) the failure to protect sufficiently against unauthorized access; (ii) the failure to conduct security investigations; (iii) the failure to restrict third-party access to its networks; (iv) the

62. *Id.*

63. *Id.* ¶ 11(a).

64. *Id.* ¶ 11(e).

65. *Id.* ¶ 11(c).

66. *Id.* ¶ 12(a).

67. Agreement Containing Consent Order, *In re* Twitter, Inc., No. 092 3093, § II (FTC June 24, 2010), available at <http://www.ftc.gov/os/caselist/0923093/100624twitteragree.pdf> [hereinafter Twitter Consent Order].

68. *Id.*; see also 16 C.F.R. § 314.4 (2010).

69. See Twitter Consent Order, *supra* note 67, § III.

70. See *In re* Dave & Buster’s, Inc., No. 082 3153 (FTC June 8, 2010) (decision and order), available at <http://www.ftc.gov/os/caselist/0823153/index.shtm> [hereinafter Decision and Order].

71. See FTC Act § 5, 15 U.S.C. § 45 (2006).

72. Complaint ¶ 5, *In re* Dave & Buster’s, Inc., No. 082 3153 (FTC June 8, 2010), available at <http://www.ftc.gov/os/caselist/0823153/index.shtm>.

73. *Id.* ¶ 8.

74. *Id.* ¶¶ 10–11.

failure to monitor outbound traffic on its networks to block unauthorized transfer of sensitive personal information; (v) the failure to limit access between in-store networks by using firewalls or other appropriate means; and (vi) the failure to limit access to its computer networks through wireless access points. Like Twitter, Dave & Buster's agreed to develop and maintain a comprehensive information security program and to have its information security program audited every other year for ten years.⁷⁵

STATE ENFORCEMENT ACTIONS

State attorneys general continue to enforce state data security laws actively. North Carolina Attorney General Roy Cooper is a prime example. Cooper entered into a consent order in May 2010 with urgent care center Prompt Med, P.A. ("Prompt Med"), settling charges that Prompt Med failed to dispose of patient records properly.⁷⁶ This action is notable because Prompt Med was held liable for the actions of a third-party service provider. In the course of its business as an urgent care center, Prompt Med collected personal information from its patients, including names, addresses, dates of birth, Social Security numbers, driver's license numbers, insurance account numbers, and personal health information.⁷⁷ Prompt Med hired an individual to dispose of those medical records, but instead of properly destroying the records, the individual disposed of about 600 files in a dumpster.⁷⁸ A third party discovered the records and turned them over to a local television station.⁷⁹ The television station notified the North Carolina Department of Justice, which charged Prompt Med with violations of North Carolina's Identity Theft Prevention Act.⁸⁰ This Act requires businesses to take reasonable measures to protect against unauthorized access to or use of personal information about North Carolina residents in connection with or after its disposal.⁸¹ Under the resulting consent order, Prompt Med agreed to pay a total of \$50,000 to the North Carolina Attorney General in the form of civil penalties, payments to the consumer protection enforcement fund, and attorney's fees and costs of the investigation and litigation.⁸²

75. See Decision and Order, *supra* note 70, § II.

76. See *North Carolina v. Prompt Med, P.A.*, No. 10cv008645 (Gen. Ct. Justice June 18, 2010) (consent judgment), available at <http://ncdoj.gov/News-and-Alerts/News-Releases-and-Advisories/Related-Information/Prompt-Med-Consent-Judgment-Granted-051810.aspx> [hereinafter Consent Judgment].

77. *Id.* at 2.

78. *Id.*

79. *Id.*

80. *Id.* at 2–3.

81. N.C. GEN. STAT. § 75-64(a) (2010) ("Any business that conducts business in North Carolina and any business that maintains or otherwise possesses personal information of a resident of North Carolina must take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal.")

82. See Consent Judgment, *supra* note 76, at 4–5.

SECURITY BREACH NOTICE LAWS

Since most states have enacted security breach notice laws, the pace of new legislation has significantly slowed. The State of Washington, however, produced an interesting development, becoming the second state to adopt a retailer liability provision.⁸³ This law provides banks, which incur significant costs due to security breaches, with a remedy against retailers and payment processors that fail to protect against a security breach.⁸⁴ When a retailer's computer system is compromised and customer credit and debit card information is subjected to unauthorized access, the bank bears the burden of reissuing credit and debit cards, changing account passwords, and taking other steps to protect affected customers from identity theft.⁸⁵ The new Washington law provides that if a payment processor or business fails to take "reasonable care" to guard against unauthorized customer account information, the payment processor or business is liable to financial institutions for the costs incurred in connection with the breach.⁸⁶ A payment processor or business is not liable if the customer account information was encrypted at the time of the breach, or if the payment processor or business was certified as compliant with the Payment Card Industry Data Security Standards.⁸⁷ It will be interesting to see whether Washington's pioneer retailer liability law will provide momentum for other states that have struggled to pass similar bills in the past.

83. See 2010 Wash. Legis. Serv. ch. 151 (HB 1149) (West) (to be codified at WASH. REV. CODE § 19.255).

84. *Id.* § 2(3)(a) ("If a processor or business fails to take reasonable care to guard against unauthorized access to account information that is in [its] possession . . . and the failure is found to be the proximate cause of a breach . . . the processor or business is liable to a financial institution for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards . . .").

85. *Id.* § 1.

86. *Id.* § 2(3)(a).

87. *Id.* § 2(2)(a) ("Processors, businesses, and vendors are not liable under this section if (a) the account information was encrypted at the time of the breach, or (b) if the processor, business, or vendor was certified compliant with the payment card industry data security standards . . .").

