

# Information Services, Technology and Data Protection

JACQUELINE KLOSEK, LINDSEY BELIER, SANTIAGO JARAMILLO CARO, DEMETRIOS ELEFThERIOU, DALE FULTON, AND MEGHAN CARR HARRIGAN

## I. Introduction

The year 2008 saw a series of interesting developments related to information services, technology, and data protection. Regulators have stepped up enforcement actions, and we have also witnessed a particular focus on data security. Certain jurisdictions are moving beyond requiring companies to notify data subjects in the event of a data security breach to requiring companies to undertake efforts to prevent security breaches.

## II. United States Federal Developments

### A. RED FLAGS RULES<sup>1</sup>

#### 1. *Overview*

Congress passed the Fair and Accurate Credit Transactions Act<sup>2</sup> (FACTA) in 2003 by adding new sections to the Fair Credit Reporting Act<sup>3</sup> (FCRA). Congress passed this act primarily to help consumers fight the growing crime of identity theft and included the directives of accuracy, privacy, limits on information sharing, and disclosure.<sup>4</sup> The Red Flags Rules (Rules) implement Sections 114 and 315 of FACTA.<sup>5</sup> Section 114 defines the entities that must comply with the Rules along with policies and procedures to identify fraudulent activities.<sup>6</sup> Section 315 requires that a user of consumer reports develop proce-

---

1. This section was written by Dale E. Fulton. Ms. Fulton is a Certified Information Privacy Professional and Senior Trainer in the Information Technology department of Goodwin Procter LLP. The author may be reached at [dfulton@goodwinprocter.com](mailto:dfulton@goodwinprocter.com).

2. Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159 (2003).

3. Fair Credit Reporting Act, 15 U.S.C. §§ 1681-81x (2008).

4. Press Release, White House, Fact Sheet: President Bush Signs the Fair and Accurate Credit Transactions Act of 2003 (Dec. 4, 2003).

5. Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 16 C.F.R. pt. 681 (2008).

6. Fair and Accurate Credit Transactions Act of 2003, sec. 114, § 1681m, Pub. L. No. 108-159, 15 U.S.C. § 1681m (2008).

dures for dealing with discrepancies to enable the user “to form a reasonable belief” that the report does, in fact, relate to the consumer for whom the report was requested.<sup>7</sup> Identity theft is defined by the Rules as “a fraud committed or attempted using identifying information of another person without authority,” consistent with the definition in FACTA;<sup>8</sup> and a victim is defined by the Federal Trade Commission (FTC) in *The President’s Identity Theft Task Force Report*, as “any person who sustained any monetary or non-monetary harm, including the theft of a means of identification, invasion of privacy, reputational damage, and inconvenience.”<sup>9</sup>

The Rules were adopted to protect consumers by requiring businesses that collect, use, maintain, or dispose of nonpublic personal information, be alert to “patterns, practices, and specific forms of activity that indicate the possible existence of identity theft.”<sup>10</sup> These businesses are required to “develop and implement a written Identity Theft Prevention Program . . . designed to detect, prevent, and mitigate identity theft.”<sup>11</sup> The deadline for mandatory compliance with the Rules for covered businesses was recently deferred from November 1, 2008, to May 1, 2009, giving those covered entities an additional six months to comply.<sup>12</sup> Although the Rule is in effect, the FTC will not enforce it until May 1, 2009.<sup>13</sup> This delay does not affect enforcement of section 315, which addresses consumer report discrepancies “or to the rule regarding changes of address applicable to [credit] card issuers.”<sup>14</sup>

## 2. *Who Must Comply?*

The Rules apply to “financial institutions” and “creditors” with “covered accounts.”<sup>15</sup> A financial institution is defined as a “[s]tate or [n]ational bank . . . savings and loan association, a mutual savings bank, . . . credit union, or any [entity] that, directly or indirectly, holds a transaction account . . . belonging to a consumer,” as defined in Title 15 of the U.S. Code.<sup>16</sup> A transaction account is a deposit or other account from which the owner makes payments or transfers.<sup>17</sup> Transaction accounts include, but are not limited to,

7. Fair and Accurate Credit Transactions Act of 2003, sec. 315, § 1681c, Pub. L. No. 108-159, § 315, 15 U.S.C. § 1681c (2008).

8. 16 C.F.R. § 681.2(b)(8) (citing 16 C.F.R. § 603.2(a) (2008)).

9. IDENTITY THEFT TASK FORCE, THE PRESIDENT’S IDENTITY THEFT TASK FORCE REPORT: COMBATING IDENTITY THEFT, at 46 (Sept. 2008), available at <http://www.ftc.gov/os/2008/10/081021taskforce-report.pdf>.

10. Fair and Accurate Credit Transactions Act of 2003, sec. 11, § 1681m, Pub. L. No. 108-159, § 114, 15 U.S.C. § 1681m (2008).

11. 16 C.F.R. § 681.2(d).

12. Press Release, Fed. Trade Comm’n, FTC Will Grant Six-Month Delay of Enforcement of “Red Flags” Rule Requiring Creditors and Financial Institutions to Have Identity Theft Prevention Programs, (Oct. 22, 2008) available at <http://www.ftc.gov/opa/2008/10/redflags.shtm> [hereinafter Six-Month Delay].

13. *Id.*

14. BUREAU OF CONSUMER PROT., FED. TRADE COMM’N, FTC ENFORCEMENT POLICY: IDENTITY THEFT RED FLAGS RULE, 16 CFR 681.2 (2008), available at <http://www.ftc.gov/os/2008/10/081022idtheftredflagsrule.pdf>.

15. 16 C.F.R. § 681.2(a)-(b).

16. 15 U.S.C. § 1681a(t) (2008).

17. 16 C.F.R. § 681.2(b)(3)(i).

checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.<sup>18</sup>

A creditor is any entity that “regularly extends, renews, or continues credit; any [entity that] regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.”<sup>19</sup> An entity that allows its customers to pay their fees or balances on a delayed payment basis would be considered a creditor. “Accepting credit cards as a form of payment does not, in and of itself, make an entity a creditor.”<sup>20</sup> Creditors include, but are not limited to, “finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.”<sup>21</sup> Where “non-profit and government entities . . . defer payment for goods or services,” they too are considered creditors.<sup>22</sup> Most creditors, except those regulated by the federal bank regulatory agencies and the National Credit Union Administration (NCUA), come under the jurisdiction of the FTC.<sup>23</sup>

A covered account is an account used mostly “for personal, family, or household purposes, that involves or . . . permit[s] multiple payments or transactions.”<sup>24</sup> A covered account is also an account for which there is a foreseeable risk of identity theft,<sup>25</sup> such as small business or sole proprietorship accounts. Covered accounts include “credit card account[s], mortgage loan[s], automobile loan[s] . . . [telecommunications accounts,] utility account[s], checking account[s], [and] savings account[s].”<sup>26</sup>

### 3. *Identifying Red Flags*

A red flag is “a pattern, practice, or specific activity that indicates the possible existence of identity theft.”<sup>27</sup> The FTC, NCUA, and federal banking agencies have issued guidelines to assist covered entities in designing their program.<sup>28</sup> These guidelines identify the five major categories of red flags as: (1) “alerts, notifications, or warnings from a consumer reporting agency;” (2) “suspicious documents;” (3) “suspicious personally identifying information,” such as a suspicious address; (4) unusual use of, or “suspicious activity relating to[,] a covered account;” and (5) “notices from customers, victims of identity theft, law enforcement authorities, or other [businesses] about possible identity theft in connection with covered accounts.”<sup>29</sup>

18. *Id.*

19. 15 U.S.C. § 1681a(r)(5) (citing 15 U.S.C. § 1691a(e) (2008)).

20. Six-Month Delay, *supra* note 12.

21. 16 C.F.R. § 681.2(b)(5).

22. Six-Month Delay, *supra* note 12.

23. 15 U.S.C. § 1681m(e)(1)(A) & (2)(A) (2008). Agencies responsible for the guidelines are: (1) the Office of the Comptroller of the Currency, Treasury; (2) the Board of Governors of the Federal Reserve System; (3) the Federal Deposit Insurance Corporation; (4) the Office of Thrift Supervision, Treasury; (5) the National Credit Union Administration; and (6) the Federal Trade Commission.

24. 16 C.F.R. § 681.2(b)(3)(i).

25. 16 C.F.R. § 681.2(b)(3)(ii).

26. 16 C.F.R. § 681.2(b)(3)(i).

27. 16 C.F.R. § 681.2(b)(9).

28. TIFFANY GEORGE & PAVNEET SINGH, FED. TRADE COMM’N, THE “RED FLAGS” RULE: ARE YOU COMPLYING WITH NEW REQUIREMENTS FOR FIGHTING IDENTITY THEFT? (2008), available at <http://www.ftc.gov/bcp/edu/pubs/articles/art10.shtm> [hereinafter THE “RED FLAGS” RULE].

29. *Id.*

#### 4. *Prevention Program*

A prevention program (program) is intended to prevent and mitigate identity theft by including appropriate responses to red flags.<sup>30</sup> Under section 114, the program must contain reasonable policies and procedures designed to identify relevant red flags and authenticate whether there is fraudulent activity.<sup>31</sup> Covered entities must incorporate these indicators into their program and respond appropriately when triggered.<sup>32</sup>

The Rules require that the covered entity's program be tailored to the size, complexity, and nature of the organization, allowing for flexible adjustment.<sup>33</sup> All programs must include certain fundamentals, such as a means of identifying, detecting, and responding to red flags.<sup>34</sup> Under section 315, users of consumer reports and any person requesting a consumer report from a consumer reporting agency, must implement a program to deal with discrepancies found between the report information and the user's record information for that consumer.<sup>35</sup> Additionally, users of the report must establish policies and procedures to notify consumer reporting agencies with the accurate information for the consumer.<sup>36</sup>

According to the Rules, there must also be a periodic review and improvement of the program with approval by appropriate committees, thereby providing the best protection to consumers. The program and any material changes to the program must be approved by the covered entity's Board of Directors or, if there is no Board, by a senior employee.<sup>37</sup> The program should include staff training, as appropriate, and provide for monitoring the work of service providers.<sup>38</sup> The program must be kept relevant and current and describe processes for implementation, review, supervision, and management.<sup>39</sup>

#### 5. *Noncompliance*

Notwithstanding the public relations implications, there are no criminal penalties for failure to comply, but financial institutions or creditors may be subject to civil monetary penalties should they violate the Rule.<sup>40</sup> Under FCRA, the FTC may bring an enforcement action and impose a civil penalty of up to \$2,500 per violation.<sup>41</sup> If noncompliance results in injury, punitive damages may be further assessed where noncompliance was willful.<sup>42</sup> With the FTC's recent enforcement of security breach incidents against such retailers as DSW, BJ's Wholesale Club, and TJX, among others, covered entities should expect the protection of nonpublic personal information.

---

30. 15 U.S.C. § 1681m(e)(1) (2008).

31. 15 U.S.C. § 1681m(e)(1)(A)-(B).

32. 15 U.S.C. § 1681m(e)(2)(A).

33. 16 C.F.R. § 681.2(d)(1).

34. 16 C.F.R. § 681.2(d)(2).

35. *See* 16 C.F.R. § 681.1(c).

36. 16 C.F.R. § 681.1(d).

37. *See* 16 C.F.R. § 681.2(b)(2)(ii).

38. 16 C.F.R. § 681 app. A(VI)(c).

39. 16 C.F.R. § 681 app. A(V).

40. THE "RED FLAGS" RULE, *supra* note 28.

41. 15 U.S.C. § 1681s(a)(2)(A).

42. *Id.*

B. FTC ENFORCEMENT ACTIONS<sup>43</sup>

In 2008, the FTC brought enforcement actions against five companies that had rendered consumers vulnerable to identity theft. The FTC targeted not only respondents' failures to maintain reasonable and adequate security programs but also their misrepresentations that personal data would be secure.

In January, the FTC issued a consent order against retailer Life is good, Inc. (Life is good) and its subsidiary. In processing sales, Life is good had collected clients' personal information, which it then stored on its network. The company had released the following privacy policy:

We are committed to maintaining our customers' privacy. We collect and store information you share with us—name, address, credit card and phone numbers—along with information about products and services you request. All information is kept in a secure file and is used to tailor our communications with you.<sup>44</sup>

The FTC claimed that such security statements were misleading because the company's security program did not maintain customers' privacy.<sup>45</sup> To the contrary, Life is good stored personal data in clear text; unnecessarily retained such information indefinitely; did not assess the risk of foreseeable attacks; and failed to implement readily-available security measures capable of preventing attacks, monitoring Internet connections to the network, and tracking unauthorized access to consumer information.<sup>46</sup> In 2006, a hacker accessed the Life is good network and, through it, the personal information of thousands of consumers.

The FTC investigated the company for unfair or deceptive practices in violation of Section 5(a) of the Federal Trade Commission Act (Section 5(a)).<sup>47</sup> The resulting settlement agreement directed Life is good "not [to] misrepresent in any manner, expressly or by implication, the extent to which respondents maintain and protect the privacy, confidentiality, or integrity of any personal information collected from or about consumers."<sup>48</sup> The company also agreed to establish and maintain a security program consisting of "administrative, technical, and physical safeguards appropriate to respondents' size and complexity, the nature and scope of respondents' activities, and the sensitivity of the personal information collected from or about consumers."<sup>49</sup> In more concrete terms, the FTC instructed the company to (i) designate an employee or employees to oversee its security program; (ii) assess security risks; (iii) design and implement reasonable risk control measures; (iv) retain a capable security provider; and (v) evaluate and adjust its program when necessary (Five Security Measures).<sup>50</sup> Finally, the settlement included bookkeeping, re-

43. This section was authored by Meghan Carr Horrigan, an associate with Goodwin Procter LLP, Exchange Place, 53 State Street, Boston, MA 02109, mhorrigan@goodwinprocter.com, (617) 570-3927.

44. Complaint at 2, *In re* Life is good, Inc., No. 072-3046 (Jan. 2008), available at <http://www.ftc.gov/os/caselist/0723046/080117agreement.pdf>.

45. *Id.*

46. *Id.*

47. Federal Trade Commission Act, 15 U.S.C. § 45(a) (2008).

48. Agreement Containing Consent Order at 3, *In re* Life is good, Inc., No. 072-3046 (Jan. 2008), available at <http://www.ftc.gov/os/caselist/0723046/080117agreement.pdf>.

49. *Id.*

50. *Id.* at 3-4.

cord-keeping, and document-production requirements and mandated biennial audits for twenty years.<sup>51</sup>

The Life is good settlement laid the framework for the FTC's other enforcement actions in 2008—four settlements with quite varied companies. First, the agency reached an agreement with Goal Financial, LLC (Goal Financial), a student loan marketer and provider. Between 2005 and 2006, respondent's employees stole the personal information of some 7,000 consumers from the company's network.<sup>52</sup> In a more devastating security breach, an employee publicly auctioned a hard-drive with the personal information of 34,000 consumers stored in clear text.<sup>53</sup>

As a financial institution, Goal Financial must comply with the Commission's Standards for Safeguarding Customer Information Rule (Safeguards Rule) and Privacy of Customer Financial Information Rule (Privacy Rule).<sup>54</sup> The Safeguards Rule requires reasonable "administrative, technical, and physical safeguards" for consumer information and mandates the Five Security Measures.<sup>55</sup> The FTC claimed that Goal Financial violated the Safeguards Rule by failing to take the outlined measures to implement a comprehensive security program. A related provision, the Privacy Rule requires financial institutions to disclose data security policies to consumers at the beginning of the relationship and annually thereafter. In attempted compliance with the regulations, Goal Financial disseminated the following statement: "Access to nonpublic personal information about you is limited to those employees who need to know such information to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information."<sup>56</sup>

The company allegedly violated the Privacy Rule and Section 5(a) by thus misinforming consumers that it maintained a reasonable security program.

The FTC's settlement with Goal Financial mirrored its settlement with Life is good except that it enjoined Goal Financial from violating the Safeguards Rule or the Privacy Rule and subjected the company to only ten years of biennial audits.

Next, the FTC announced a settlement agreement with ValueClick, Inc. (ValueClick) and its wholly-owned subsidiaries, Hi-Speed Media, Inc. and Babylon, Inc. Respondents use Internet advertisements to connect consumers with online merchants. Consumers must then provide personal information to purchase goods. ValueClick pledged to protect personal information through "industry standard security measures," such as encryption, but stored some consumer data without encryption and used a nonstandard form of encryption for other data.<sup>57</sup> Between 2005 and 2006, hackers infiltrated the ValueClick sites. Respondent allegedly could have prevented the breach through readily-available or inexpensive security solutions.

---

51. *Id.* at 4-6.

52. Complaint at 2, *In re* Goal Financial, LLC, No. 072-3013 (Mar. 2008), available at <http://www.ftc.gov/os/caselist/0723013/080304complaint.pdf>.

53. *Id.*

54. Safeguards Rule, 16 C.F.R. pt. 314 (2002); Privacy Rule, 16 C.F.R. pt. 313 (2000). Both rules implement the Gramm-Leach Bliley Act, 15 U.S.C. § 6801-6809 (1999).

55. 16 C.F.R. pt. 314.

56. Complaint at 3, *In re* Goal Financial, LLC, No. 072-3013.

57. Complaint at ¶¶ 38-42, *United States v. ValueClick, Inc.*, No. CV08-0171 (2008), available at <http://www.ftc.gov/os/caselist/0723111/080317complaint.pdf>.

The FTC investigated ValueClick under Section 5(a), again for misrepresenting its security program to consumers and failing to take appropriate measures to protect personal information. The settlement included a record \$2.9 million and an order permanently enjoining the company from misrepresenting the manner or extent of its security programs.<sup>58</sup> The incorporated consent order further required ValueClick to implement a comprehensive security program including the Five Security Measures, to submit to biennial independent audits, and to comply with bookkeeping, recordkeeping, and document production provisions.<sup>59</sup>

Finally, the FTC reached simultaneous settlements with mammoth data-collection corporation Reed Elsevier, Inc. (REI) and its subsidiary, Seisint, Inc. (Seisint), and with international retailer TJX Companies, Inc. Seisint compiles consumer data, including nonpublic information, in commercial databases. Authorized customers, often employers and landlords, access the system through a User ID and password. At the time of the security breach, the system allowed clients to use a common word as a User ID or password, establish an identical User ID and password, share credentials as a group, and store credentials on cookies on personal computers.<sup>60</sup> The system never prompted users, even those with access to highly confidential data, to change credentials and did not require information transmitted over the system to be encrypted.<sup>61</sup>

Hackers obtained user credentials, accessed the database, and acquired the personal information of more than 300,000 consumers. The FTC claimed that REI's security program failed to protect sensitive consumer information, caused or was likely to cause substantial injury to consumers, and was thus an unfair act or practice in violation of section 5(a).<sup>62</sup>

Meanwhile, the FTC investigated TJX Companies, Inc. (TJX) after an infamous breach of the retailer's network compromised the personal information of 455,000 consumers. TJX allegedly failed to protect customer information acquired on its computer network in the course of business. Specifically, TJX used clear text to store and transmit consumer information; did not employ readily available security measures to limit unauthorized access, wireless or otherwise, to the network; did not require network users to supply strong passwords or different passwords to access different programs; and failed to detect or prevent security breaches.<sup>63</sup> The FTC charged the company with unfair business practice under section 5(a) because its failure to provide adequate protection for personal information had caused or was likely to cause substantial harm to consumers.<sup>64</sup>

In both the TJX and Seisint settlements, the companies agreed to implement and maintain comprehensive security systems, in part through the Five Security Measures; to submit to biennial audits for twenty years; and to comply with bookkeeping and record-

---

58. Stipulated Final Judgment at 6-8, *United States v. ValueClick, Inc.*, No. CV08-0171 (C.D. Cal. 2008), available at <http://www.ftc.gov/os/caselist/0723111/080317judgment.pdf>.

59. *Id.* 9-16.

60. Complaint at 3-4, *In re Reed Elsevier Inc.*, No. 052-3094 (FTC 2008), available at <http://www.ftc.gov/os/caselist/0523094/080327complaint.pdf>.

61. *Id.* at 4.

62. *Id.* at 5.

63. Complaint at 2, *In re TJX Companies, Inc.*, No. 072-3055 (FTC 2008), available at <http://www.ftc.gov/os/caselist/0723055/080327complaint.pdf>.

64. *Id.* at 3.

keeping standards.<sup>65</sup> According to FTC Chairman Deborah Platt Majoras, enforcement actions against companies that have failed to safeguard consumer data should send a clear message that “[i]nformation security is a priority for the FTC, as it should be for every business in America.”<sup>66</sup>

### C. PROPOSED REGULATION<sup>67</sup>

During 2008, attention continued to be directed to the issue of online behavioral advertising. Behavioral advertising, also known as behavioral targeting, is a widespread practice used by web publishers, Internet marketers, and service providers to track consumer activities online and serve up more targeted content to consumers. Behavioral advertising is an important component of many companies’ marketing strategies but has come under fire due to privacy concerns. Over the past few years, the FTC and state regulators have been studying the issue and proposing guidelines and draft regulations.<sup>68</sup> While lawmakers and regulators continue to debate the issue, a new lawsuit, filed in the Northern District of California on November 10, 2008, may play a significant role in determining the future of behavioral advertising.<sup>69</sup>

Behavioral advertising uses technology to anonymously track and tabulate consumer clicks in order to understand an individual consumer’s online activities. Cookies are used to monitor and track web surfing habits including the websites visited, the length of time spent on a given web page, and the content viewed. While the consumer information collected may not seem to be personally identifiable, as it does not identify individuals by name or address, the practice has the ability to collect and aggregate extensive amounts of personal information. The inventory of data collected by behavioral advertising is analyzed in order to predict a consumer’s future behavior and target future advertising to that consumer based on their web surfing history.

Among its benefits, behavioral advertising allows marketers and service providers to specifically target more relevant content and advertisements to a given individual’s interests and potentially, reduce unwanted advertising. But many fear that the vast repository of information stored about individual consumers, often without their knowledge or consent, may be easily misappropriated for unintended purposes. The privacy implications of this unregulated practice are particularly worrisome when the tracking involves children or other sensitive personal information about a consumer’s health or finances.

In response to consumer privacy concerns raised by behavioral advertising, the FTC has spent the last decade investigating, studying, and enforcing privacy developments. As part of its efforts to protect online consumer privacy, the FTC has hosted several events that

65. Complaint at 3-4, *In re* Reed Elsevier Inc. No. 052-3094 (Mar. 2008), available at <http://www.ftc.gov/os/caselist/0523094/080327complaint.pdf>; Agreement Containing Consent Order, *In re* TJX Companies, Inc., No. 072-3055 (Mar. 2008), available at <http://www.ftc.gov/os/caselist/0723055/080327agreement.pdf>.

66. Press Release, Fed. Trade Comm’n, Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers’ Data (Mar. 27, 2008), available at <http://www.ftc.gov/opa/2008/03/datasec.shtm>.

67. This section was authored by Jacqueline Klosek and Lindsey Bleier. Ms. Klosek is Senior Counsel and Ms. Bleier is an Associate with Goodwin Procter LLP, New York.

68. See *infra* notes 68-74.

69. See Complaint, *Valentine v. Nebuad, Inc.*, 2008 WL 5085988 (N.D. Cal. Nov. 10, 2008) (No. 3:08-cv-05113).

brought consumers together with consumer and privacy advocates, government representatives, and Internet companies including a three-day public hearing titled *Protecting Consumers in the Next Tech-ade* in the fall of 2006<sup>70</sup> and a Town Hall Meeting titled *Behavioral Advertising: Tracking, Targeting, and Technology* in the fall of 2007.<sup>71</sup> These discussions culminated in a set of draft guidelines, *Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles*, which were issued by the FTC in December 2007.<sup>72</sup>

The proposed guidelines express the FTC's optimism that privacy concerns raised by behavioral advertising can be addressed and monitored by self-regulation.<sup>73</sup> The critical questions underlying the draft FTC guidelines focus on which principles should determine what kinds of ads users see on the Internet, and where. Specifically, the draft guidelines propose that:

- Any website collecting data for the purpose of behavioral advertising must provide clear notice of the practice and obtain express consumer consent before collecting any data.
- If a website intends to use such data in any way that materially differs from the manner described at the time of collection, that website must obtain affirmative express consumer consent before using that data for behavioral advertising purposes.
- Any business that collects or stores data for behavioral advertising purposes must undertake reasonable security measures to protect that data and to maintain such data for a reasonable period of time necessary to fulfill a legitimate business purpose or to support a specific law enforcement need.<sup>74</sup>

During the summer of 2008, the FTC held congressional hearings on the subject, and the FTC continues to solicit comments from all interested parties on the draft guidelines.<sup>75</sup> The FTC is interested in determining whether the data collected is being used for secondary purposes other than behavioral advertising and, if so, whether such secondary uses would require additional levels of protection.<sup>76</sup>

While lawmakers and regulators consider the issues surrounding behavioral advertising, a lawsuit filed on November 10, 2008, may determine that Internet service providers (ISPs) must seek consumer's affirmative consent before selling personal consumer information to advertising companies before Congress even decides to pass legislation on the issue. A group of fifteen internet users (and potentially millions more) seeking class action status filed suit in federal district court in California against behavioral targeting company NebuAd and twenty-six internet service providers.

NebuAd developed an advertising system centered on its patented hardware that purchased information from ISPs about individual users' internet activity in order to send

70. See Press Release, Fed. Trade Comm'n, FTC Staff Proposes Online Behavioral Advertising Privacy Principles (Dec. 20, 2007), available at <http://www.ftc.gov/opa/2007/12/principles.shtml>.

71. *Id.*

72. *Id.*

73. *Id.*

74. *Id.*

75. See Press Release, Fed. Trade Comm'n, FTC Testifies on Behavioral Advertising (July 9, 2008), available at <http://www.ftc.gov/opa/2008/07/behaviorialad.shtml>.

76. See Press Release, Fed. Trade Comm'n, FTC Staff Extends Comment Period for Proposed Online Behavioral Advertising Principles; Commission Approves Final Consent Orders in Matters of Milliman, Inc. and Ingenix, Inc. (Feb. 12, 2008), available at <http://www1.ftc.gov/opa/2008/02/fyi08003.shtml>.

web users targeted ads. After Congress learned of NebuAd's platform in the summer of 2008, Congress launched an investigation into NebuAd's behavioral targeting and related involvement with ISPs.<sup>77</sup> Part of that investigation involved a formal inquiry sent to thirty-three Internet companies "[i]n order . . . to better understand how companies may be engaged in efforts to target Internet advertising, the impact of such efforts on consumers, and broader public policy implications."<sup>78</sup> The six ISPs named in the NebuAd suit each responded to the Congressional inquiry that they had tested NebuAd's platform on a trial basis.<sup>79</sup>

The lawsuit alleges that the defendants violated the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and California's Invasion of Privacy Act and Computer Fraud Law, as well as aiding and abetting, civil conspiracy, and unjust enrichment. The plaintiffs allege that:

[t]he collection of data by the NebuAd device was wholesale and all-encompassing [and that] [l]ike a vacuum cleaner, everything passing through the pipe of the consumer's internet connection was sucked up, copied, and forwarded to the California processing center. Regardless of any representations to the contrary—all data—whether sensitive, financial, personal, private, complete with all identifying information, and all personally identifying information, was recorded and transmitted to the California NebuAd facility.<sup>80</sup>

While the suit does note that ISPs are permitted to track some user activity to monitor for viruses, spam, and the overall health of their networks, it also alleges that NebuAd's Deep Packet Inspection technology goes beyond that permissible purpose. The suit further alleges that the ISP's current Acceptable Use Policies do not inform subscribers that their web activities might be sold to advertisers and, rather, that "such 'opt out' rights were misleading, untrue, and deceptive."<sup>81</sup>

The lawsuit notes that the defendants acted both independently and jointly to access and disclose sensitive, personally identifiable information about ISP subscribers.<sup>82</sup> In addition, the suit alleges that the interception of such information was intentional, without users' knowledge or consent, and not in the normal course of business.<sup>83</sup> The lawsuit alleges, rather, that the ISPs' activities exceeded their authorization access and control of users' private information concerning users' web communications and that such activity was for the sole purpose of increasing profitability and advertising revenues.<sup>84</sup>

It will be very important to monitor the outcome of this case. If NebuAd fails to defend this suit successfully, ISPs may be required to obtain users' affirmative consent before selling user information to third parties. Furthermore, ISPs and advertisers will need to

---

77. Complaint at ¶ 89, *Valentine v. NebuAd*, 2008 WL 5085988 (N.D. Cal. Nov. 10, 2008) (No. 08 Civ. 5113).

78. *Id.* (quoting Letter from House Commerce & Energy Comm.).

79. *Id.* at ¶ 90 (quoting Bresnan Communications Response).

80. *Id.* at ¶ 82.

81. *Id.* at ¶ 87.

82. *Id.* at ¶ 3.

83. *Id.* at ¶¶ 3-4.

84. *Id.* at ¶ 122.

invent new ways to monetize their users' data as it is unlikely that users' will provide the affirmative consent required by a potential plaintiff victory.

### III. State Developments

#### A. DATA SECURITY AND BREACH NOTIFICATION<sup>85</sup>

"Every business, whether large or small, must take reasonable and appropriate measures to protect sensitive consumer information, from acquisition to disposal. [The Federal Trade Commission] will continue to prosecute companies that fail to fulfill their legal responsibility to protect consumers' personal information."<sup>86</sup>

##### 1. *Generally*

The number of data breaches reported through 2008 easily outpace the number of breaches in all of 2007.<sup>87</sup> In addition to the increasing number of breaches, the numerous state security breach notification laws, which currently number over forty, as well as the several pending federal bills addressing security breach notification, indicate that this is an increasingly significant data protection issue for the entities that experience the breaches as well as for the individuals who are victims of such breaches.<sup>88</sup> There is no question that data security practices will continue to be under increased scrutiny and that companies must have adequate measures in place to safeguard personal data. But a company that has implemented advanced and cutting-edge technology to protect data can still experience a data security breach. Companies should take appropriate actions not only to prevent security breaches, but also to have mechanisms in place to send security breach notifications in the most expedient time possible in the event there is a breach that triggers notification. Interestingly, however, although we continue to see an increasing number of security breaches, the extent to which fraud can be accurately attributed to a particular data breach remains unclear.

##### 2. *Data Security*

From a federal standpoint, there are sectoral laws that require companies to safeguard personal information.<sup>89</sup> Even if companies are not subject to a federal sectoral law requiring data security, however, companies must still safeguard personal information (1) from an industry or customer expectation standpoint and (2) from a FTC perspective, as they

---

85. This section was authored by Demetrios Eleftheriou of the General Counsel's Office at American Express.

86. Press Release, Fed. Trade Comm'n, Company Will Pay \$50,000 Penalty for Tossing Consumers' Credit Report Information in Unsecured Dumpster (Dec. 18, 2007) (quoting Chairman Deborah Platt Majoras), available at <http://www.ftc.gov/opa/2007/12/aumort.shtm>.

87. See *Identity Theft Resource Center, ITRC 2008 Breach List*, [http://www.idtheftcenter.org/artman2/publish/lib\\_survey/ITRC\\_2008\\_Breach\\_List.shtml](http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml) (last visited Mar. 15, 2009).

88. For list of legislation requiring notification of security breaches involving personal information, see *National Conference of State Legislatures, State Security Breach Notification Laws*, <http://ncsl.org/programs/lis/cip/priv/breachlaws.htm> (last visited Mar. 4, 2009) [hereinafter *State Security Breach Notification Laws*].

89. See, e.g., Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999); Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

could face potential enforcement action by the FTC for engaging in an unfair or deceptive trade practice.<sup>90</sup> Like in prior years, the FTC has brought enforcement actions in 2008 against companies for failing to adequately protect personal data.<sup>91</sup>

From a state standpoint, Massachusetts passed a comprehensive data security law in 2008, which requires companies to have a written and comprehensive information security program to protect the personal information of Massachusetts residents.<sup>92</sup> Under the new law, companies must encrypt all personal data, including data transmitted wirelessly and over the Internet, and data stored on portable devices such as jumpdrives and blackberries. In addition, this new law requires companies to obtain from third-party service providers a written certification that such third parties have a written, comprehensive information security program that complies with the new rule.<sup>93</sup> Like California and its pioneering security breach notification law, the new Massachusetts law could serve as a model for other states and trigger a flurry of comprehensive state data security laws over the next few years. As for other states, Nevada requires encryption as of October 1, 2008.<sup>94</sup> Specifically, under the Nevada law, businesses “shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.”<sup>95</sup> Connecticut also passed a new law that would make businesses liable for an intentional failure to properly protect or dispose of personal data.<sup>96</sup>

### 3. *Data Security Breach Notification*

As of November 2008, forty-four states and the District of Columbia have security breach notification laws on the books.<sup>97</sup> Given the large number of state security breach laws, many companies are asking for a federal law that would streamline and preempt the inconsistent notification approach brought on by the state laws. Although several federal security breach notification bills were introduced in the 110th Congress, none are expected to pass. We expect to see the new 111th Congress introduce similar security breach notification bills, but it is unclear whether such legislation will pass in 2009. Even if a federal law does pass, a federal law that does not fully preempt inconsistent state laws, unfortunately, will simply be another law to add to the hodge-podge of state notification laws and continue to create compliance headaches for businesses.

90. See Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2008).

91. For list of enforcement actions, see Federal Trade Commission, Enforcement, [http://ftc.gov/privacy/privacyinitiatives/promises\\_enf.html](http://ftc.gov/privacy/privacyinitiatives/promises_enf.html) (last visited Mar. 4, 2009).

92. See 201 MASS. CODE REGS. 17 (2008). The original deadline to comply with the Massachusetts data security law was January 1, 2009; however, Massachusetts will phase in the compliance deadline—May 1, 2009, for general compliance and January 1, 2010, for encrypting portable devices, such as jumpdrives.

93. See *id.*

94. See NEV. REV. STAT. § 597.970 (2008).

95. See *id.*

96. See 2008 Conn. Acts page no. 167 (Reg. Sess.). Under the new Connecticut law, businesses could be subject to fines of up to \$500,000. This new law took effect on October 1, 2008.

97. See State Security Breach Notification Laws, *supra* note 88.

## B. RFID<sup>98</sup>

The use of Radio Frequency Identification (RFID) to track individuals is a particularly sensitive issue, and accordingly, several states have addressed or attempted to address the issue through legislation. Legislators, at least in twenty states, introduced privacy legislation relating to the use of RFID in 2008, but only a few notable bills were passed at the state level.<sup>99</sup> Reacting to concern over the possibility of human RFID implantation, a new California law in effect since January 1, 2008, regulates the implantation of RFIDs and other identification devices in humans.<sup>100</sup> California's new law creates a private right of action for individuals implanted with a subcutaneous identification device in violation of this new law including civil actions for actual damages, compensatory damages, punitive damages, injunctive relief, and any other appropriate relief. Notably, California's legislation does not prohibit or otherwise address the use of RFID in clothing or other wearable objects whether known or unknown to the person wearing it.<sup>101</sup>

## C. COPPA ENFORCEMENT ACTIONS<sup>102</sup>

When Congress enacted the Children's Online Privacy Protection Act (COPPA),<sup>103</sup> the primary goal was to place parents in control of what personally identifiable information (PII) was collected from their young children while online. COPPA sets forth a framework of practices that governs the collection of, access to, and use of PII by websites that are directed toward children. COPPA mandates strict requirements concerning parental oversight and consent on behalf of their children. Among other requirements, COPPA requires a commercial website operator to meet specific requirements prior to collecting, using, or disclosing PII from children. All of the requirements are to increase the level of parental involvement. Specifically, under COPPA, the website operator must: (1) provide clear, understandable, and complete notice of its information practices, including specific disclosures directly to the parent when required by COPPA; (2) obtain verifiable parental

98. This section was authored by Lindsey Bleirer, an Associate with Goodwin Procter.

99. See National Conference of State Legislators, 2008 Privacy Legislation Related to Radio Frequency Identification (RFID), <http://www.ncsl.org/programs/lis/privacy/rfid08.htm> (last visited Mar. 4, 2009).

100. CAL. CIV. CODE § 52.7 (West 2009).

101. The "persons" covered by California law include "individual[s], business association[s], partnership[s], limited partnership[s], corporation[s], limited liability compan[ies], trust[s], estate[s], cooperative association[s], or other entit[ies]." CAL. CIV. CODE § 52.7(h)(2) (West 2009). This is particularly notable in light of the pending case in California in which parents from Sutter, a small town California, contacted the American Civil Liberties Union (ACLU) of Northern California in 2005 after their daughters returned from their public middle school with new identification badges that appeared to have an embedded microchip. For more information about Sutter, see Press Release, ACLU of Northern California, Privacy Rights are at Risk—Parents and Civil Liberties Groups Urge School District to Terminate Use of Tracking Devices (Feb. 7, 2005), available at [http://www.aclunc.org/news/press\\_releases/privacy\\_rights\\_are\\_at\\_risk\\_-\\_parents\\_and\\_civil\\_liberties\\_groups\\_urge\\_school\\_district\\_to\\_terminate\\_use\\_of\\_tracking\\_devices.shtml](http://www.aclunc.org/news/press_releases/privacy_rights_are_at_risk_-_parents_and_civil_liberties_groups_urge_school_district_to_terminate_use_of_tracking_devices.shtml). See also Press Release, ACLU of Northern California, Victory for Students, Parents and Civil Liberties Groups—Company Announces it will End Tracking Pilot Program (Feb. 16, 2005), available at [http://www.aclunc.org/news/press\\_releases/victory\\_for\\_students\\_parents\\_and\\_civil\\_liberties\\_groups\\_-\\_company\\_announces\\_it\\_will\\_end\\_tracking\\_pilot\\_program.shtml](http://www.aclunc.org/news/press_releases/victory_for_students_parents_and_civil_liberties_groups_-_company_announces_it_will_end_tracking_pilot_program.shtml).

102. This section was authored by Jacqueline Klosek, Senior Counsel with Goodwin Procter LLP, New York, and Dale E. Fulton, a Certified Information Privacy Professional and Senior Trainer in the Information Technology department of Goodwin Procter LLP.

103. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 (2008).

consent prior to collecting, using, or disclosing PII from children; (3) give parents the option to consent to the collection and internal use of their children's PII without consenting to the disclosure of that information to third parties; and (4) provide a reasonable means for parents to review the information collected from their children and to prohibit the further use of such information.

COPPA has been enforced vigorously at the federal level by the FTC, but COPPA also empowers the states' attorneys general to bring civil action on behalf of state residents. This power recently came to the forefront of public attention when the Texas Attorney General brought COPPA-related enforcement actions against three out-of-state companies. The three websites in the Texas actions had parental consent features that were easily manipulated and by-passed with relative ease by savvy children. While the Texas Attorney General elected to pursue enforcement actions against these three sites, arguably, many sites are in the same position in that they are relying upon features that can be circumvented. Due to the lack of reasonable controls, children were allowed to access various features of these websites without parental knowledge.

Texas Attorney General Abbott claimed Santa.com<sup>104</sup> collected a wide range of PII such as: first and last name; home or other physical address including street name and name of a city or town; e-mail address or other online contact information, including but not limited to an instant messaging user identifier or a screen name that reveals an individual's e-mail address; telephone number; social security number; persistent identifier such as a customer number held in a cookie; combination of a last name or photograph of an individual with other information such that the combination permits physical or online contacting; or information concerning the child or the parents of that child.

The second website to receive attention from the Texas Attorney General was Gamesradar.com.<sup>105</sup> Gamesradar.com is a website designed for people with an interest in video games. The website includes content or allows access to content inappropriate for children along with games clearly targeted to young children such as Disney's *Chicken Little*, *Ice Age*, and *Cars*. To access certain features of the website, one must register by providing certain PII, including first and last name, e-mail address, physical address, gender, and date of birth chosen from a drop-down menu. The menu, however, only allows a selection from years prior to 1995, thereby not allowing the visitor to select an age that would make him/her younger than thirteen. Thus, if a ten-year-old child born in 1998 attempts to register, the closest birth year that could be selected would be 1994, indicating a current age of thirteen.

TheDollPalace.com<sup>106</sup> also caught the attention of the Texas Attorney General. At TheDollPalace.com website, children create and play with web-based dolls, including sexually explicit dolls. To use features or participate in activities of the website, children are required to register. Activities, such as participating in chat rooms, are encouraged by offering "doll points," which may then be used to purchase items on the website. Registering entails providing first and last name, e-mail address, and date of birth, state, zip code, country, and gender. Accessing additional website features requires a profile be

---

104. *Texas v. Small's Seed Co.*, No. 07 Civ. 002600 (W.D. Tex. Dec. 18, 2007).

105. Complaint, *Texas v. Future Us, Inc.*, 2007 WL 4817985 (W.D. Tex. Dec. 5, 2007) (No. 07 Civ. 987).

106. Complaint, *Texas v. Doll Palace Corp.*, WL 4817946 (W.D. Tex. Dec. 5, 2007) (No. 07 Civ. 988, 2007).

filled out that consists of a ten page questionnaire including detailed PII such as height, weight, eye color, details about personal habits, and whether the child has their own computer or Internet access only in a public location. The child is asked questions about the type of person they are interested in meeting, for example, age importance, including the option of meeting someone older as well as those within five miles of their location. This PII is easily accessed by other members of the website. The website's parental permission page requires only a click "OK" for the child to register, allowing easy circumvention of COPPA consent requirements. Additionally, parental consent is requested after collection of the child's PII has already taken place. The permission page does not provide the parent with website operator contact information, the option to review and revoke consent, or specify the type of information collected.

While the Texas actions are notable as they represent the first state-based enforcements of COPPA, it is important to recognize that the federal authorities also remain active in investigating and enforcing COPPA violations. The recent FTC enforcement action against imbee.com,<sup>107</sup> a social networking website directed to kids ages eight to fourteen, collects PII from children as defined in COPPA. After providing their PII, the child is able to post text, photographs, and graphics to their personal page, which is kept private until the child's parent has completed the registration process. But, according to the FTC, if the parent failed to complete the registration process, imbee.com nonetheless continued to maintain the child's data. Additionally, according to the FTC, imbee.com failed to disclose to the parent that their child's PII had already been collected and failed to provide the parent the right to review or have their child's information deleted. Furthermore, imbee.com's privacy policy failed to disclose that imbee.com would use the child's personal information to mail the child "imbee cards" bearing the child's name, address, photo, imbee name, and imbee profile page URL.

These recent cases emphasize the critical importance of ensuring that one's web operations comply with COPPA requirements. Companies that fail to comply with the requirements of COPPA risk not only fines but also damage to their brand reputation and business. In the above cases, injunctions were sought against the defendants along with damages, restitution, or other compensation. A court can hold violators of COPPA liable for civil penalties of up to \$11,000 per violation. The amount of the penalty may turn on a number of factors including the egregiousness of the violation, the number of children involved, the size of the company, the amount and type of PII collected, how the information was used, and whether it was shared with third parties. Fines in FTC actions have been increasing steadily, beginning with injunctive relief in some of the earlier cases and progressing to the most recent fine of one million dollars in the Xanga.com case.

---

107. Complaint, United States v. Industrious Kid, Inc., 2008 WL 243658 (N.D. Cal. filed Jan. 28, 2008) (No. 08 Civ. 639).

#### IV. International Developments<sup>108</sup>

Since 1991, Colombia's exiguous data protection regime was based on Article 15 of the Colombian Constitution<sup>109</sup> and the jurisprudence issued by the Constitutional Court, which was mainly based on controversial issues involving financial data and credit reports.

After years of struggling and controversy, early this year, Congress finally passed a bill regulating data protection in Colombia. Because of the special constitutional nature of this bill, a previous review by the Constitutional Court was needed. Through a ruling dated October 16, 2008,<sup>110</sup> the Colombian Constitutional Court upheld the Data Protection Bill (the Bill). Consequently, very soon, Colombia will have a regulation on the matter, which unfortunately cannot be considered as a comprehensive statute as regards data privacy.

Even though in principle the Bill applies to the gathering and transfer of all kinds of data concerning natural or legal persons, it really focuses mainly in the conditions for protection and processing of financial data, the latter of which is understood to mean information related to operations involving monetary transactions in trade, commerce, financial services, credit, and transfer of data to and from third countries.

The Bill introduces several principles that must be observed upon the collection, gathering, usage, and transfer of data. Said principles<sup>111</sup> are more or less similar to those provided under the European Union (EU) Directives or the ones set forth in the Organization for Economic Co-operation and Development (OECD) guidelines, the Asia-Pacific Economic Cooperation (APEC) principles, and the Code of Fair Information Practices.

Three kinds of data are described and regulated in the Bill: (i) public data, regarded as information considered as public by law or by constitutional mandate, such as public records; (ii) semi-Private data, understood as private information of general interest, such as financial data; and (iii) private data, which relates to the information reserved to the intimate sphere of the person, such as sexual preferences and personal interests.

---

108. Santiago Jaramillo Caro is a Partner at Gómez-Pinzón Zuleta Abogados S.A. He may be reached for comment at [sjaramillo@gpzlegal.com](mailto:sjaramillo@gpzlegal.com). The author wishes to recognize the significant collaboration of Miguel Villamizar in the research and drafting of this section.

109. Article 15 provides:

Every individual has the right to personal and family intimacy and to his/her good reputation, and the State will respect them and have these rights and ensure they are respected. Similarly, individuals have the right to know, update, and rectify information gathered about them in data banks and in records of public and private entities. Freedom and other guarantees approved in the Constitution will be respected in the gathering, handling, and circulation of data. Correspondence and other forms of private communication are inviolable. They may only be intercepted or recorded pursuant to a court order, following the formalities established by law. For tax or legal purposes and for cases of inspections, supervision, and intervention of the state, the submission of accounting records and other private documents may be required within the limits provided by law.

Constitution De Politica Columbia art. 15 (Colom.) (unofficial translation), *available at* <http://confinder.richmond.edu> (emphasis added).

110. Ruling No. C-1011 of 2008.

111. These principles apply to all kinds of data (public, semiprivate, or private) and are: i) accuracy of data; ii) end use of data; iii) limited circulation of data; iv) limited availability of data; v) integral interpretation of constitutional rights; vi) data security; and vii) data confidentiality.

The Bill regulates and applies mainly to the activities performed by *data sources*, *data administrators*, and *data users*.

*Data sources* collect data from data owners and must: i) guarantee the accuracy and truthfulness of the data submitted to data administrators and users; ii) give notice and obtain previous consent for the usage of data from data owners;<sup>112</sup> iii) keep the data updated; iv) rectify inaccurate information; v) limit the circulation of data to the scope requests made by administrators; vi) receive and solve claims from data owners; vii) inform the data administrator of any pending claims over the accuracy of data; and viii) comply with all the instructions issued by the control governmental authority.

*Data administrators* gather, process, keep, and distribute data directly collected or received from data sources. Data administrators must, *inter alia*: i) guarantee accessibility to data owners as well as the possibility to update, rectify, or modify the information when inaccurate or false; ii) allow limited access and circulation of the data under the conditions authorized by the data owner; iii) request from the data source the authorization for usage issued from the data owner, when legally required; iv) undertake security measures to protect the data; and v) comply with all the instructions issued by the control governmental authority.

*Data users* receive the information from data administrators and must: i) keep the data confidential and only use it according to the authorization given; ii) inform the data owner of the use given to the information; iii) safeguard the conditions of data protection; and iv) comply with all the instructions issued by the control governmental authority.

Both data users and data administrators must comply with additional specific regulation concerning operational issues in Colombia and transfer of data.

The new Bill introduces timeframes for the availability of the so-called “negative financial data”<sup>113</sup> in data bases. The general rule is that negative data shall only remain in databases twice as long as the time during which the debtor was delinquent, without exceeding four years. As an exception to the time-frame availability and as an incentive for delinquent debtors to pay their default obligations, the Bill includes a grace period of six months once the law becomes enforceable. Upon payment of debts and obligations, negative financial records must be erased from databases.

The Bill has quite a few controversial articles. Among them, Article 5(f) deals with international transfer of data. This article provides, *inter alia*, that data can be transferred to international databanks under the law without the consent of the data owner in those cases provided as long as the data controllers and data processors verify that foreign laws provide similar guarantees and rights to the owner of the data.

On the other hand, the Bill states that the Superintendent of Finance and the Superintendent of Industry and Commerce shall perform controlling and surveillance data protection activities. These entities belong to the central government and cannot really be deemed as privacy authorities, at least under the terms and conditions as such authorities are understood in the United States, Canada, and Europe.

---

112. The Bill provides that such consent is not necessary in case of collection and transfer of the “financial data” (as defined in the Bill). But the Constitutional Court seemed to clarify that notice and consent was needed in all cases. At the time of writing of this article, Ruling No. C-1011 is still pending official publication.

113. Data concerning delay in financial payments or credit obligations.

Even though a data protection regulation has been requested by some sectors in Colombia for years, the new regulation is far from becoming a comprehensive data privacy statute. The Bill does not regulate data privacy in key sectors, such as labor (workplace privacy), health, pensions, education, and children's information usage. And the new regulation involving commercial and financial activities has already raised comments, questions, and concerns from companies that could qualify as data administrators or users.

In the following months, we should expect special regulation and decisions from the Superintendent of Finance and the Superintendent of Industry and Commerce. We hope that this gives clarity and confidence in the gathering and transfer of data.

Colombia made a major step with this new regulation. But the road ahead looks quite confusing and controversial.