Information Services, Technology, and Data Protection

NICHOLAS D. WELLS, POORVI CHOTHANI, AND JAMES M. THURMAN*

I. Information Services and Technology

A. REVISED FEDERAL TRADE COMMISSION GUIDES, CONSUMER PROTECTION, AND SOCIAL NETWORKING*

The year 2009 saw the continuing growth of social networking or social media sites as an increasingly important tool for both business and personal communication.[1] Sites such as Facebook, Twitter, LinkedIn, and others are commonly referred to in business-to-consumer communications; thousands of blog websites permit individuals to post publicly-visible commentary or other information. Maintaining an online presence by one or more of these methods is considered *de rigueur* by many individuals.[2]

With this growing trend, concerns have arisen regarding risks to consumers when the line between individual action and commercial action is unclear. Such activity is known by names such as "Word of Mouth Marketing" and "Social Media Marketing." Some estimates place annual expenditures on such advertising approaches at $40 million to $60 million.[3] For example, when a blogger posts a review of a product, consumers may assume that the individual is uninterested and that the review represents his or her true

---

* Nicholas D. Wells served as Editor of the Information Services, Technology, and Data Protection Committee's 2009 YIR contribution. He is the principal of Wells IP Law, LLC and a consultant attorney at General Electric in trademarks and advertising law. Poorvi Chothani is a founder and managing member of LawQuest, a law firm in Mumbai, India, and is also admitted to the New York State Bar and as a Solicitor in England and Wales. James M. Thurman is a J.D. Research Fellow with the DETECTER Project on the faculty at the University of Zurich.

* Contributed by Nicholas D. Wells.

1. Forrester Research predicts a compound annual growth rate in social media-based advertising of 34% from 2008 through 2014. *See generally* Andy Beal, *Forrester Predicts Huge Growth for Social Media Marketing*, Apr. 24, 2004, http://www.marketingpilgrim.com/2009/04/forrester-social-media-growth.html (predicting a compound annual growth rate in social media-based advertising of 34% from 2008 through 2014).

2. *See, e.g.*, Kevin Anderson, *New York Times Names First Social Media Editor*, GUARDIAN, May 26, 2009, http://www.guardian.co.uk/media/pda/2009/may/26/new-york-times-twitter.

3. *See* Letter from Gary Ruskin, Executive Director, Commercial Alert, to Donald Clark, Secretary, FTC 6 (Oct. 18, 2005), *available at* http://www.commercialalert.org/buzzmarketing.pdf (citing Matthew Creamer, *Is Buzz Marketing Illegal? Lawyers Warn of Advertising Law Disclosure Requirements*, ADVERTISING AGE, Oct. 3, 2005).

opinions. In fact, the content of the review may have been influenced by the blogger receiving a free product or a payment from the manufacturer of the product being reviewed. Indeed, many companies now consult with entities to assist them with securing "sponsored" communications within a social media environment.[4] Industry participants have grappled with this issue for several years.[5]

After lengthy consideration, the U.S. Federal Trade Commission (FTC) in October 2009 revised its Guides Concerning the Use of Endorsements and Testimonials in Advertising (the Guides).[6] The Guides have been updated to reflect the public's current reliance on social networking and social media and reduce consumer confusion regarding commercial speech.

As in previous versions of the Guides, the revised Guides discuss the meaning of an endorsement: a communication that constitutes a type of advertising message because it reflects the views or opinions of a sponsoring entity rather than the person making the communication.[7] But unlike prior versions, the revised Guides provide extensive examples drawn from social media, with particular attention to personal blogs.[8] The Guides state that to avoid potential liability under the Federal Trade Commission Act, any person or entity acting as an endorser (as defined in the Guides) or where there is a "material connection" between an endorser and the seller of an advertised product must make certain disclosers to inform readers or viewers that the statement is an endorsement.[9] Such disclosures may take the form of statements that a commercial entity has provided free product or a payment to the person making a statement.[10]

Importantly, the Guides state that where an endorser (such as a person posting to a personal blog) makes false or unsubstantiated statements, both the blogger and the commercial entity that the blogger is endorsing may be held liable by the FTC.[11] Because many commercial entities regularly provide free promotional merchandise to encourage reviews (hopefully favorable), this dual liability raises the specter of commercial entities investing significant time and money to police the activities of bloggers to whom they have provided free products.

While legal experts generally have agreed that the lack of transparency in "commercialized" social media presented a potential risk to consumers, reaction among bloggers has been mixed, often owing to a lack of understanding regarding (among other things) federal rule-making procedures under the Administrative Procedures Act, the enforcement

4. *See, e.g.*, IZEA, http://izea.com (last visited Jan. 25, 2010) (consulting on "sponsored tweets" and "blog marketing).

5. The National Advertising Division of the Council of Better Business Bureaus, Inc. and its affiliate, the Electronic Retailing Self-Regulation Program, previously attempted to develop standards for word of mouth marketing to deal with a number of issues raised by advertisers or consumers. *See, e.g.*, Cardo Systems, Case Report No. 4934, (NAD Case Reports Nov. 14, 2008).

6. FTC Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255 (2009), *available at* http://www2.ftc.gov/os/2009/10/091005revisedendorsementguides.pdf. *See also* Press Release, Federal Trade Commission, FTC Publishes Final Guides Governing Endorsements, Testimonials (Oct. 5, 2009), http://www2.ftc.gov/opa/2009/10/endortest.shtm.

7. 16 C.F.R. § 255(b).

8. *See, e.g., id.* § 255(e) exs. 8, 16; *see also id.* § 255.1(d) ex. 5.

9. *See* 16 C.F.R. § 255.5.

10. *See id.* exs. 4, 7.

11. *See id.* § 255.1(d).

role of the FTC, and the true scope of the definitions set forth in the Guides. The FTC stated that, to date, it has never instituted an action against a consumer endorser (as a blogger would likely be characterized), and never expects to do so.[12] Nevertheless, Randall Rothenberg, President and Chief Executive Officer of the influential Interactive Advertising Bureau, has penned an open letter to the FTC calling on it to repeal the Guides, calling into question their constitutionality.[13]

B. Developments in Online Security and E-Privacy Law in India*

Information technology (IT) and IT-enabled services have made significant contributions to India's economic growth. The proliferation of the Internet and the use of the World Wide Web are global, but India's economic dependence on it is unique. However, India does not have specific laws pertaining to privacy or data protection. The Information Technology Amendments of 2008 (the Amendments) to the Information Technology Act, 2000[14] (the IT Act) contain some provisions that apply to privacy and data protection. The Amendments[15] passed on December 23, 2008, received the assent of President of India on February 5, 2009, and came into "effect" only when they were "notified" on October 27, 2009.[16]

The absence of data protection laws in India acts as a serious impediment to the growth of certain industries. To establish credibility, some companies have obtained certification to confirm their compliance with international regulations like The Sarbanes Oxley Act and the Healthcare Insurance Portability and Accountability Act.[17]

The Constitution of India enshrines Fundamental Rights and guarantees to every citizen a "right to life and personal liberty" but does not specifically protect privacy.[18] The Supreme Court had interpreted "personal liberty" to include a "Right to Privacy."[19] In recent times, the IT Act has been interpreted to give some protection. Currently, the Amendments make it a violation of a person's privacy to intentionally or knowingly capture, publish, or transmit the image of a private area of a person without his or her con-

12. Joe Ciarallo, *FTC Clarifies Blogger Guidelines: 'We've Never Brought a Case Against Somebody Simply for Failure to Disclose,'* PRNewser, Oct. 8, 2009, http://www.mediabistro.com/prnewser/social_networks/ftc_clarifies_blogger_guidelines_weve_never_brought_a_case_against_somebody_simply_for_failure_to_disclose_139589.asp.

13. *See* Letter from Randall Rothenberg, President and Chief Executive Officer, Interactive Advertising Bureau, to Jon Leibowitz, FTC Chairman (Oct. 15, 2009), *available at* http://www.iab.net/insights_research/public_policy/openletter-ftc.

* Contributed by Poorvi Chothani, Esq.

14. The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, *available at* http://mit.gov.in/download/itbill2000.pdf [hereinafter IT Act].

15. The Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009, *available at* http://mit.gov.in/download/it_amendment_act2008.pdf [hereinafter IT Act of 2000 (as amended)].

16. *See* Press Release, Ministry of Commc'n & Info. Tech., Information Technology (Amendment) Act, 2008 Comes Into Force (Oct. 27, 2009), http://pibmumbai.gov.in/scripts/detail.asp?releaseId=E2009PR1153.

17. Delhi Quality Services is one example of a company providing such certification services to Indian companies. *See* Delhi Quality Services, http://www.dqsindia.com/compliance-services/sox-sarbox-act-sarbanes-oxley-act-compliance-services.php (last visited Jan. 26, 2010).

18. India Const. art. 21, *available at* http://lawmin.nic.in/coi/coiason29july08.pdf (providing that "[n]o person shall be deprived of his life or personal liberty except according to procedure established by law.").

19. Kharak Singh v. State of U.P., (1964) 1 S.C.R. 332, ¶ 21.

sent.[20] While the protections provided by this new provision are admirable, they remain fundamentally inadequate in an electronic age, where personal data is more likely to comprise facts rather than images.[21]

Additionally, the Amendments impose a punishment and a penalty for identity theft described as the dishonest "use of the electronic signature, password or other identification feature of any other person."[22] The Amendments also include a punishment for cheating by impersonation with the use of a "communication device or computer."[23]

The Amendments give the regulatory authorities the right to block or access data that is stored on or available through a computer resource.[24] These rights expose personal and business communications to government access in the name of national security, giving the authorities wide power with the risk of misuse, thus further jeopardizing an individual's privacy.

The IT Act describes data as "a representation of information, knowledge, facts, concepts or instructions" but does not identify personal data per se.[25] The Amendments describe offenses, including data theft, and a reference to sensitive personal data, that invoke a penalty of up to three years imprisonment and/or a fine. The term "sensitive personal data" is described as "such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations . . . ."[26] The Amendments introduce the concept of data theft as a punishable offense.[27] The Amendments provide that a person can be liable for penalties of up to three years imprisonment when dishonestly receiving electronic information.[28] The element of *mens rea* is important to prove that the information was received "dishonestly" and the receiver knew it was "stolen."[29]

Prior to the Amendments, the IT Act only addressed breach of confidentiality and privacy by the government or its agencies. The 2008 Amendments specifically include provisions permitting criminal prosecution of others (intermediaries)[30] for offenses that include disclosure "without consent" or "in breach of lawful contract."[31] Importantly, the Amendments require intermediaries, such as ISPs, to preserve and retain information as prescribed by the government. Any intermediary who intentionally or knowingly fails to do so may be subject to a fine or imprisonment.[32]

---

20. *See* IT Act of 2000 § 66E (as amended).

21. This provision may be compared in some aspects to statutory and common law right of publicity in effect in many states and the personality rights protected in many countries.

22. *See* IT Act of 2000 § 66C (as amended).

23. *See id.* § 66D.

24. Section 69A permits government authorities to block public access to information through any computer resource; Section 69B permits government authorities to monitor and collect traffic data or other information through any computer resource for purposes of "Cyber Security." *See id.* § 69A.

25. IT Act § 2(1)(o).

26. IT Act of 2000 § 43A (as amended).

27. *Id.* § 43.

28. *Id.* § 66B.

29. *See, e.g.*, India Pen. Code (1860), § 378 (making intent an important element of the offense).

30. The definition of this term in Section 2(1)(w) is very broad and includes, for example, Internet Service Providers. IT Act of 2000 § 2(1)(w) (as amended).

31. *Id.* § 72A.

32. *Id.* § 67C(2).

The Amendments also specify penalties for violations, while establishing levels of compensation for aggrieved parties and granting the authority to implement the provisions of the IT Act.[33] The provisions, introduced by the Amendments and pertaining to "Cyber Security," address the need for the physical security of devices as well as for the content or information stored on these devices.[34] They also provide protection from unauthorized access, use, disclosure, disruption, modification, and destruction. Newly added provisions also make the "theft" of computers or other communication devices an offense.[35]

The 2008 Amendments to the IT Law in India provide measures that will benefit individuals and protect data, while increasing the liability of service providers and intermediaries. These changes will provide an element of comfort to entities that outsource work to India.

II. Data Protection

A. U.S. Federal Developments*

1. *Continuing Efforts to Pass Federal Data Protection and Data Breach Legislation*

Data privacy advocates continue pressing for a federal data protection act that would provide some level of protection for personal data beyond the piecemeal protection now provided by federal law.[36] These efforts have included promoting a federal data security breach notification act that would—at a minimum—preempt any conflicting provisions within the existing state laws addressing this topic.[37] Some oppose federal legislation, either because they fear government involvement in data management on the scope now found in the European Union, or because they believe a federal standard could provide only a minimum standard, to which existing state laws would in many cases, add further state-specific requirements.

Despite repeated failed attempts at passing such legislation at the federal level, support appears to be growing. In November 2009, Senator Patrick Leahy's bill, the Personal Data Privacy and Security Act of 2009, was reported out of the Senate Judiciary Committee—after failing to progress during the previous two sessions of Congress—and will proceed to the full Senate.[38] If passed in its current form, the bill would require data brokers and companies to establish and implement data privacy and security programs and would give individuals access to, and the opportunity to correct, any of their personal informa-

33. *Id.* § 43.

34. *Id.* § 2(i)(nb).

35. *Id.* § 66B.

* Contributed by Nicholas D. Wells.

36. For example, federal laws protect personal health information (via the Health Insurance Portability and Accountability Act) and personal financial data (via the Gramm-Leach-Bliley Act), yet no comprehensive federal or state law governs the collection, processing, and use of all forms of personal data. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 1173(d)(2), 110 Stat. 1936 (1996); Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 502, 113 Stat. 1338 (1999).

37. Jon Oltsik, *Why a National Data Breach Notification Law Makes Sense*, CNET News, Apr. 14, 2009, http://news.cnet.com/8301-1009_3-10219135-83.html.

38. GovTrack.US, S. 1490: Personal Data Privacy and Security Act of 2009, http://www.govtrack.us/congress/bill.xpd?bill=s111-1490 (last visited Jan. 28, 2010).

tion held by commercial data brokers.[39] The bill also includes criminal penalties for intentionally concealing a security breach that exposes personal data.[40]

On the same day Senator Leahy's bill was reported out, the Data Breach Notification Act, a bill sponsored by Senator Dianne Feinstein of California, was also reported out of the Senate Judiciary Committee after several failed attempts.[41] The Data Breach Notification Act is more limited in scope than the Personal Data Privacy and Security Act of 2009. The Data Breach Notification Act would require U.S. agencies and businesses that engage in interstate commerce to report data breaches to victims whose personal information has been, or is reasonably believed to have been, compromised.[42] It would also require agencies and businesses to report large data breaches to the U.S. Secret Service.[43] Some privacy advocates have objected to the provisions of the Data Breach Notification Act because it may still permit some level of "self-policing" where businesses decide for themselves whether a data breach rises to the level of seriousness that it should be reported to the U.S. Secret Service. Yet the implementation of a federal data breach notification law—even one with flaws—is seen by many industry participants as a significant improvement over the current piecemeal requirements of state-by-state data breach notification laws.[44]

It remains to be seen how the full Senate will respond to the proposed bills in light of various industry and political pressures.

2. *New Breach Notification Requirements under the Health Insurance Portability and Accountability Act*

The Federal Trade Commission and the Department of Health and Human Services released interim final rules that became effective September 23, 2009, requiring health plans and others handling employees' health data (both Covered Entities and Business Associates) to comply with sweeping changes in data breach notification requirements related to personally identifiable medical data.[45]

While the Health Insurance Portability and Accountability Act already included a Privacy Rule governing how personal medical information could be processed those subject to the Act, the new rules require that every violation of the Privacy Rule (breach) be documented and reviewed to determine the likely level of harm that the violation may cause to the affected individuals.[46] If appropriate, the entity holding the personal information must then notify the individual about the incident and the Department of Health

39. S. 1490, 111th Cong. §§ 2 & 201 (2009), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:s1490rs.txt.pdf

40. *Id.* § 102.

41. GovTrack.us, S. 139: Data Breach Notification Act, http://www.govtrack.us/congress/bill.xpd?bill=s111-139 (last visited Jan. 28, 2010).

42. S. 139, 111th Cong. § 2 (2009), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:s139is.txt.pdf.

43. *Id.* § 7.

44. *See, e.g.*, Grant Gross, *Senate Panel Approves Data-Breach Notification Bills*, COMPUTERWORLD, Nov. 6, 2009, *available at* http://computerworld.co.nz/news.nsf/scrt/6402CA6D786CBA34CC25766500775C35 (noting that industry leading security software provider Symantec supports the Data Breach Notification Act).

45. Breach Notification for Unsecured Protected Health Information; Interim Final Rule, 45 C.F.R. § 160, 164 (2009), *available at* http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf.

46. *Id.*

and Human Services.[47] The Department has stated that it will not impose sanctions on entities that fail to notify affected individuals for Privacy Rule violations occurring between September 23, 2009 and February 20, 2010. Nevertheless, all such violations must be logged as of the effective date of the interim final rules. Some exceptions and safe harbors are provided in the rule. For example, encrypted data need not be considered as compromised because it is not available to an attacker even if other security measures are breached.[48]

B. U.S. STATE LAW DEVELOPMENTS*

1. *New State Data Breach Notification Laws*

On July 1, 2009, new data security breach laws took effect in Alaska and South Carolina.[49] On August 28, 2009, a new data security breach law also took effect in Missouri.[50] With these new laws, only five states remain that do not have laws controlling key aspects of data security, including, most prominently, rules and procedures for notifying a person whose personal or financial data has potentially been comprised.[51]

Provisions of the new laws in Alaska, South Carolina, and Missouri mirror those in most other states having data breach notification laws. Each requires businesses to notify individuals of security breaches whenever an unauthorized person acquires unencrypted computerized personal information that the business reasonably deems likely to cause harm to the affected persons.[52] The Alaska law also requires notification if paper records are disclosed containing personal information.[53] In some cases, businesses may also be required to notify a state Attorney General's office, or state office of consumer protection.[54]

The new laws in Alaska, South Carolina, and Missouri also require notification to the three national credit-reporting bureaus under certain circumstances, such as when data of

47. *See generally* Erin Brisbay McMahon, *Sweeping New Data Breach Regulations Impact Healthcare Industry, Employers with Self-Insured Plans, and Vendors, Health Care Law Update*, Wyatt, Tarrant, & Combs, LLP, Sept. 2009, http://wyattemployment.files.wordpress.com/2009/09/data-breach-article1.pdf; Stuart D. Levi, et al., *HIPAA Update: HHS Issues Draft Data Security Guidelines and FTC Proposes Rule on Notification of Security Breaches*, Skadden, Arps, Slate, Meagher & Flom LLP & Affiliates, May 26, 2009, http://www.skadden.com/content%5CPublications%5CPublications1798_0.pdf.

48. *See generally* McMahon, *supra* note 47; Levi, *supra* note 47.

* Contributed by Nicholas D. Wells.

49. *See* ALASKA STAT. § 45.48.010 (2008), *available at* http://www.legis.state.ak.us/PDF/25/Bills/HB0065Z.PDF; S.C. CODE ANN. § 39-1-90 (2008), *available at* http://www.scstatehouse.gov/code/t39c001.htm.

50. H.B. 62, 95th Gen. Assem., Reg. Sess. § 407.1500 (Mo. 2009), *available at* http://www.house.mo.gov/billtracking/bills091/billpdf/truly/HB0062T.PDF.

51. The five states that do not have a data security breach notification law are Alabama, Kentucky, Mississippi, New Mexico and South Dakota. Washington D.C., Puerto Rico, and the U.S. Virgin Islands, along with forty-five states, do have such laws in effect. Nat. Conf. of State Legis., State Security Breach Notification Laws, As of Dec. 9, 2009, http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx (last visited Jan. 29, 2010).

52. ALASKA STAT. § 45.48.010; S.C. CODE ANN. § 39-1-90; H.B. 62 § 407.1500 (2).

53. ALASKA STAT. § 45.48.080 (b)(1); S.C. CODE ANN. § 39-1-60; H.B. 62 § 407.1500 (2)(8).

54. *See generally International Security Breach Notification Survey*, Foley & Lardner LLP and Eversheds LLP, Nov. 2009, http://www.govexec.com/nextgov/1109/securityBreachTable.pdf.

more than 1,000 residents is involved in a breach.[55] All three states provide significant civil penalties for businesses that fail to comply with legal requirements.[56]

2. *Data Breach Enforcement*

Despite the provisions of an increasing number of relevant laws, the past year saw a continuing pattern of data breaches—both large and small.[57] Significant litigation in this area is also moving ahead, and in a few cases, is reaching its conclusion.

The U.S. Department of Veterans Affairs has settled a class-action lawsuit resulting from a 2006 data breach incident in which a laptop and external drive belonging to a Veterans Affairs' analyst was stolen, potentially exposing the names, dates of birth, and Social Security numbers of about 26.5 million active duty troops and veterans to identity theft.

Under the terms of the settlement, the Department of Veterans Affairs has agreed to pay $20 million to anyone able to show that they were harmed by the data loss, with individual payments as high as $1,500. In this case, the thieves who stole the laptop were apprehended by the FBI, and no evidence was found that any personal data had actually been compromised.

Individuals are also seeking to impose liability on financial institutions that fail to ensure adequate security of financial account credentials.

In February 2007, an attacker used the username and password of an account holder at Citizens Financial Bank to log on and initiate an advance on the account owner's home equity credit line, eventually transferring $26,500 to the attacker's bank in Austria.[58] In August 2009, a federal judge permitted the account owners to go forward with a suit against Citizens Financial and let a jury decide whether the bank's online security was sufficient.[59] The judge noted that, contrary to federal guidelines, Citizen's Financial was only using single-factor authentication on the account that was attacked.

Similarly, a construction firm in Sanford, Maine, filed suit against Ocean Bank, a division of People's United Bank, alleging that Ocean Bank failed to take adequate security precautions to prevent attackers from transferring approximately $588,000 from the firm's account over an eight-day period in May 2009.[60]

Litigation continues to move forward as multiple parties seek to impose liability on other firms who have suffered large data breaches.

Two class action lawsuits were filed in Georgia and Ohio based on a data breach that occurred at Royal Bank of Scotland (RBS) Worldpay, which allegedly included personal information and social security numbers of more than one million individuals who used

55. ALASKA STAT. § 45.48.040; S.C. CODE ANN. § 39-1-90 (K); H.B. 62 § 407.1500 (2)(8).

56. ALASKA STAT. § 45.48.080 (b)(1); S.C. CODE ANN. § 39-1-60; H.B. 62 § 407.1500 (2)(8).

57. *See generally* Chronology of Data Breaches, Privacy Rights Clearinghouse, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Feb. 2, 2010).

58. Shames-Yeakel v. Citizens Fin. Bank, No. 07-C-5387 (N.D. Ill. Aug. 21, 2009).

59. *See* Shames-Yeakel v. Citizens Financial Bank: Failure to Expeditiously Implement State-of the Art Security Measures Can Create Liability for Negligence in Data Breach Cases (Sept. 2, 2009), http://www.digitalmedialawyerblog.com/2009/09/shamesyeakel_v_citizens_financ.html.

60. *See* Complaint at 1-2, Patco Construction Co. v. People's United Bank, No. 09-CV-00503 (Me. Dist. Ct. Oct. 9, 2009), *available at* http://voices.washingtonpost.com/securityfix/Complaint%20091809.pdf.

payroll cards or gift cards issued by the defendants.[61] The two suits have now been consolidated and are moving forward in the Northern District of Georgia.[62]

In relation to the same RBS Worldpay data breach, prosecutors announced in late 2009 that four men had been indicted for allegedly hacking into RBS Worldpay systems and using their payment card systems to steal over $9 million from ATMs during a twelve-hour period in November 2008.[63]

Civil and criminal suits have been proceeding in relation to the massive data breach of the Heartland Payment Systems that occurred in late 2008. Multiple civil suits have been consolidated in federal court in Houston. At about the same time, the hacker behind the Heartland Payment Systems attack pleaded guilty to charges in a nineteen-count indictment that included conspiracy, wire fraud, and aggravated identity theft.[64] Under a plea agreement, the defendant will serve between fifteen and twenty-five years for multiple data breach charges and will be fined as much as $250,000 for each of the charges. Heartland Payment Systems to date has spent more than $13 million on costs related to the data breach.[65]

C. EUROPEAN DEVELOPMENTS—SWITZERLAND*

Several important issues were addressed during 2009 by the Swiss Federal Data Protection Commissioner, and illustrate the data protection issues faced in many European jurisdictions.

1. *Logistep Case—IP Addresses as Personal Data*

Perhaps the most significant development with respect to Data Protection Law in Switzerland this year was a case which the Federal Data Protection Commissioner (the Commissioner) brought before the Federal Administrative Court against the Swiss company Logistep AG.[66] Logistep was in the business of providing information to copyright owners about users of peer-to-peer (P2P) file-sharing services who shared copyrighted content for download via the services' networks. Logistep obtained information about users by permitting them to download a particular copyrighted work and collecting the data associated with the connection that the user established to download that file.[67] This informa-

61. Class Action Defense Cases—*In re* RBS Worldpay: Judicial Panel On Multidistrict Litigation (MDL) Grants Defense Motion To Centralize Class Action Litigation In Northern District Of Georgia, http://classactiondefense.jmbm.com/2009/10/class_action_defense_casesin_r_162.html (Oct. 2, 2009).

62. *Id.*

63. Thomas Claburn, *Four Indicted In $9 Million RBS WorldPay Hack*, INFO. WEEK, Nov. 11, 2009, *available at* http://www.informationweek.com/news/software/showArticle.jhtml?articleID=221601284.

64. Jaikumar Vijayan, *Gonzalez Pleads Guilty to TJX, Other Data Heists*, COMPUTER WORLD, Sept. 11, 2009, *available at* http://www.computerworld.com/s/article/9137900/Gonzalez_pleads_guilty_to_TJX_other_data_heists.

65. Jaikumar Vijayan, *Lawsuits over Heartland Data Breach Folded into One*, COMPUTER WORLD, Oct. 5, 2009 *available at* http://www.computerworld.com/s/article/9138947/Lawsuits_over_Heartland_data_breach_folded_into_one.

* Contributed by James M. Thurman.

66. Bundesverwaltungsgericht [BGer] [Federal Court] May 27, 2009, A-3144 Logistep AG [ATF] 1 (Switz.), *available at* http://jumpcgi.bger.ch/cgi-bin/JumpCGI?id=27.05.2009_A-3144/2008.

67. *See id.* ¶ A.

tion was then supplied to Logistep's client to assist in any case for copyright infringement that the client might wish to pursue. A key factor in identifying individuals who shared copyrighted works via the P2P file-sharing services was the Internet Protocol (IP) Addresses of the relevant P2P users.[68]

The court adopted the view of the Article 29 Working Group that IP-Addresses that refer to an identifiable individual constitute personal data. The court noted that even dynamic IP-Addresses essentially became personally identifying once the commencement of a criminal investigation permitted Logistep's clients to request that Internet Service Providers (ISPs) determine which user had been assigned the address at a particular time.[69] Ultimately, the court determined that Logistep's actions would have the tendency to routinely violate Article 4(4) of the Swiss Data Protection Act, which required that the acquisition of personal data as well as the purpose behind the processing of that data be cognizable for the data subject. Here, Logistep's collection of data was not readily apparent to P2P network users.[70] The court also held that Logistep violated Article 4(3), which required that the processing of personal data be limited to those purposes which had been indicated previously, were obvious under the circumstances, or had been legally provided. No existing legal provision explicitly permitted private parties to collect data concerning copyright infringers on P2P networks. Because Logistep's activities relied on the fact that P2P users were not aware that it was collecting data, it could neither be said that those users had been made aware of Logistep's purposes for collecting data or that those purposes were obvious under the circumstances.[71]

Despite the fact that the court determined that Logistep's activities violated two aspects of Swiss Data Protection Law, the court held that the violation was permissible, since overwhelming public and private interests in upholding copyright law and the rights of the copyright holder justified the violation.[72] Since IP-Addresses did not qualify as sensitive data under Article 3(c)(4) of the Swiss Data Protection Act, Logistep had no duty to seek the permission of P2P network users.[73] The Commissioner has appealed the case to the Federal Court—the highest court in Switzerland.[74]

2. *Google Street View—Preserving Online Privacy*

The year 2009 also saw Google's extension of its Street View service to Switzerland.[75] A number of citizens, however, complained to both Google and the Commissioner about the failure of Google to adequately encrypt faces and license plates that were visible online via the Street View service. After a closer examination, the Commissioner also discovered that Street View included images of areas that generally would not be visible to street pedestrians—areas such as private driveways and walled gardens. On September 11, 2009, the Commissioner recommended that Google take certain actions to ensure adequate pro-

68. *See id.* ¶ 2.2.2.
69. *Id.* ¶ 2.2.4.
70. *Id.* ¶¶ 9.3.4 - 9.3.6.
71. *Id.* ¶ 10.3.2.
72. *Id.* ¶ 12.3.2.
73. *Id.* ¶ 9.3.6.
74. *Datenschützer zieht Fall Logistep weiter*, 20 MINUTEN, June 29, 2009, http://www.20min.ch/digital/webpage/story/13245355.
75. *See* Google Maps, http://maps.google.ch/.

tection of privacy: develop better methods to ensure complete encryption of faces and license plate numbers; pay particular attention to preserving privacy within sensitive areas, such as hospitals, schools, and prisons; delete images taken of private driveways where the owner had not provided permission; delete images of enclosed areas and lower the Street View camera for future filming; announce one week prior to shooting as well as one week prior to uploading images which areas and communities would be filmed; and refrain from taking additional pictures of Swiss streets until legal issues had been resolved. Reportedly, Google worked to improve its encryption technology to obscure faces and license plate numbers. Google, however, found the requests to provide notice of filming one week in advance and to lower the Street View camera problematic. The weather made it difficult to know a week in advance whether filming could take place, and lowering the camera would place more emphasis on pedestrian faces rather than on the surrounding buildings and streets.[76] As a result of Google's refusal to comply with all of the Commissioner's recommendations, the Commissioner brought action against Google in the Federal Administrative Court.[77] In December, the Commissioner's Office announced that Google had agreed not to upload any additional material from Switzerland to Street View until the Court had reached a decision. Under the agreement, however, Google is free to continue photographing within Swiss territory at its own risk.[78] As of the date of this publication, the case is still pending.

3. *Social Networking Sites and Internet Dragnets*

Other themes that have received significant attention from the Commissioner are social networking sites and internet dragnets conducted by the police. The Commissioner has made a campaign of warning the public regarding the privacy dangers that social networking sites pose and called upon government authorities to exert more pressure for site providers to improve transparency for users.[79] He expressed particular concern for young people and suggested that schools should incorporate programs to raise awareness of the risks of revealing personal information on social networking sites.[80]

The privacy issues arising from internet-conducted police dragnets have gained attention as local police agencies within Switzerland have begun to place the photos of soccer "hooligans"—individuals who behave in a disorderly fashion or commit acts of violence at sporting events—on the internet in the hope of receiving the public's help in making

76. *Google widersetzt sich dem Datenschützer*, TAGES-ANZEIGER, Oct. 15, 2009, http://www.tagesanzeiger.ch/digital/internet/Google-widersetzt-sich-dem-Datenschuetzer/story/30881514.

77. Press Release, Federal Data Protection Commissioner, Street View: EDÖB zieht Google vor Bundesverwaltungsgericht (Nov. 13, 2009), http://www.news-service.admin.ch/NSBSubscriber/message/de/30087.

78. Press Release, Federal Data Protection Commissioner, Vereinbarung in Sachen Google Street View (Dec. 17, 2009), http://www.news-service.admin.ch/NSBSubscriber/message/de/30822.

79. *Das Internet vergisst nie*, NEUE ZÜRCHER ZEITUNG, June 29, 2009, http://www.nzz.ch/nachrichten/schweiz/datenschutz_soziale_netzwerke_1.2846147.html.

80. *Schulfach: Die Risiken des Internets*, BASLERZEITUNG, June 30, 2009, http://bazonline.ch/schweiz/standard/Schulfach-Die-Risiken-des-Internets/story/27839218.

arrests. The Commissioner has expressed the opinion that, in order to be in conformity with the principle of proportionality, such photos should only be displayed when the individual has committed a serious offence.[81]

81. *Ein Richter sollte Internet-Fahndung anordnen*, 20 MINUTEN, July 2, 2009, http://www.20min.ch/news/schweiz/story/19696158.