Survey of the Law of Cyberspace: Introduction

*By Jonathan T. Rubens and Kristine F. Dorrain**

When ABA President Laurel Bellows announced she would make cybersecurity one of her major areas of focus,[1] members of the Cyberspace Law Committee noted the rapidly increasing demand for practical guidance and commentary on cybersecurity along with other cyberlaw issues that the committee's members have long studied. For over fifteen years the committee has offered this survey[2] along with articles, informational websites, CLE programming, and a diverse set of books and model agreements on the areas where the cyberworld and business law intersect. The existence of a separate area of law known as cyberspace law or cyberlaw may remain questionable: for years we have said: "[C]yberspace law is most often just the application of old, time-tested laws applied to new technologies and situations."[3] Yet, as the internet, technology, and cyberworld issues now feature prominently in the practice of every lawyer, and most businesses, the work of the committee has never been more relevant to business law practice.

In this year's survey, as before, short pieces written by experts who apply the law to the context of cyberspace highlight some of the more notable legislative and judicial developments from the past year. Our aim is to bring the developments in the law pertaining to cyberspace to a practical level, useful for every business lawyer. We survey cases and developments, not noting every change, but highlighting the ones our committee believes should not be overlooked based on their applicability and significance. This year we present fifteen dis-

* Jonathan Rubens is the chair of the Cyberspace Law Committee and is co-founder of Javid Rubens LLP in San Francisco, where his practice focuses on commercial transactions, startups and emerging companies, and intellectual property protection. He regularly advises entrepreneurs and investors on new venture formation, represents businesses and investors in equity financings, mergers, and acquisitions, and acts as outside general counsel advising businesses on a wide variety of commercial transactions and IP issues. Kristine F. Dorrain is Director of Internet and IP Services at Forthright and manages the domain name dispute resolution program for the National Arbitration Forum; she now serves as Programs Director for the Committee.

We thank Forthright for providing law clerks Stephanie Morales (attorney), Steven Kinsella (attorney), Paula Polasky, Chantal Trinka, and Cassie Hanson to edit and cite-check the survey.

1. *New ABA President Will Advocate for Gender Equity, Among Other Issues*, ABANOW.ORG (Aug. 31, 2012), http://www.abanow.org/2012/08/new-aba-president-will-advocate-for-gender-equity-among-other-issues/.

2. Julia Gladstone, *Survey of the Law of Cyberspace: Introduction*, 53 BUS. LAW. 217 (1997).

3. Michael F. Fleming & Kristine F. Dorrain, *Survey of the Law of Cyberspace: Introduction*, 66 BUS. LAW. 155, 155 (2010).

tinct, shorter pieces with four of them authored by lawyers making their first contribution to *The Business Lawyer*.

In keeping with the ABA President's focus on cybersecurity, our survey begins with developments in cybersecurity and continues the discussion through its close cousin, data privacy, featuring two pieces from European Union authors, then concluding with an update on where the United States is on data privacy. We weave our contribution on payments into this mix, as the managing and processing of electronic payments has significant security and privacy implications.

First, Roland Trope launches our cybersecurity focus with "*There's No App for That": Calibrating Cybersecurity Safeguards and Disclosures*.[4] Mr. Trope presents an unvarnished account of the dangers of technology that develop faster than the security protocols needed to protect consumers and highlights some of the risks faced by companies that experience a breach. We then transition to a piece by Theodore F. Claypoole and Richard C. Balough that focuses on the impact geolocational technology has on privacy and personal Fourth Amendment protections.[5] A bifurcated discussion of how the European Union treats privacy and the collection and dissemination of personal data, particularly facial and biometric identification data, is led by Mr. Gregory Voss from France,[6] then followed by a related discussion of how the European Union has developed the law surrounding "cookies"—the information tracked from internet browsing sessions—in a survey prepared by Robert Bond from the United Kingdom.[7] Ms. Fatima Khan presents the view from the United States, highlighting efforts made by the Federal Trade Commission to protect consumer privacy, both through enforcement actions and recommendations.[8] And finally, Professor Sarah Jane Hughes brings us her expertise on what is going on regarding payments, particularly as affected by cyberspace, including e-payments and credit card regulation, electronic funds transfer, and credit card fees.[9]

We transition to more of a business law focus with Timothy Chorvat and Laura Pelanek's update of last year's piece on electronically stored information in litigation.[10] Mr. Chorvat and Ms. Pelanek focus on discovery of information in social media and provide an update on technological measures courts have implemented to streamline discovery. Just as we began to feel last year that there could not possibly be any more to update with respect to electronic con-

4. Roland L. Trope, "*There's No App for That": Calibrating Cybersecurity Safeguards and Disclosures*, 68 BUS. LAW. 183 (2012).

5. Theodore F. Claypoole & Richard C. Balough, *Developments in the Law Concerning Geolocational Privacy*, 68 BUS. LAW. 197 (2012).

6. W. Gregory Voss, *Survey of Recent European Union Privacy Developments*, 68 BUS. LAW. 205 (2012).

7. Robert Bond, *The EU E-Privacy Directive and Consent to Cookies*, 68 BUS. LAW. 215 (2012).

8. Fatima Nadine Khan, *Survey of Recent FTC Privacy Enforcement Actions and Developments*, 68 BUS. LAW. 225 (2012).

9. Sarah Jane Hughes, *L'Embarras du Choix: A Year of Developments in the Laws Affecting Remittance Transfers, Credit Cards, and Certain Prepaid Cards*, 68 BUS. LAW. 233 (2012).

10. Timothy J. Chorvat & Laura E. Pelanek, *Electronically Stored Information in Litigation*, 68 BUS. LAW. 245 (2012); *see* Timothy J. Chorvat & Laura E. Pelanek, *Electronically Stored Information in Litigation*, 67 BUS. LAW. 285 (2011).

tracting, the courts surprised us with new cases involving clickthrough and browsewrap agreements. Deborah Boykin provides us with an overview of the new cases, finding that the law remains stable, even as the courts continue to be confronted with disputes.[11] Regarding other website-related updates, Michelle Boldon's survey on the ethics of attorney advertising using "deal of the day" channels focuses on the recommendations of the handful of bar associations that have grappled with the issue.[12] Finally, Phillip Schmandt advises business lawyers on the new EU Model Interoperability Agreement for Transmission and Processing of Electronic Invoices and Other Business Documents.[13] While primarily applicable in the European Union, the model agreement is also likely to be used for international businesses trading with EU corporations and is highly relevant.

The final batch of survey articles address in detail the business of the internet and legal implications for doing business online, particularly related to the protection of intellectual property. Phong Nguyen reprises his survey of patent law for the fourth year with cases discussing patentable subject matter as well as warning of the danger of public disclosure.[14] Cathy Gellis continues to follow developments in website owner liability for user generated content, particularly focusing on how courts are defining a web host for the purposes of the statute, and how much control the web host has to exercise before it is found liable.[15] Cheryl Balough focuses her survey on false advertising and how not only the courts, but class action plaintiffs and the Federal Trade Commission, have taken action to address serious internet-related breaches.[16] Kristine Dorrain and Jon Rubens pair up to provide a brief overview of a few trademark and copyright cases, focusing on topics such as keyword advertising, software copyrights, and litigation trends.[17] Also addressing trademark law, but even more so in cyberspace, survey author Leland Gardner updates his work from last year with recent cases brought under the Anticybersquatting Consumer Protection Act and the Uniform Domain Name Dispute Resolution Policy.[18] Mr. Gardner focuses on the definition of bad faith intent to profit and the protection of personal names in cyberspace.

This survey covers some, but by no means all, of the areas covered by the subcommittees of the Cyberspace Law Committee. If you are interested in learning more about the work of the committee, please visit our website at http://www.abanet.org/dch/committee.cfm?com=CL320000.

11. Deborah Davis Boykin, *Survey of E-Contracting Cases: Browsewrap, Clickwrap, and Modified Clickwrap Agreements*, 68 Bus. Law. 257 (2012).

12. R. Michelle Boldon, *The Ethics of Lawyers Marketing Their Services on Daily Deal Websites*, 68 Bus. Law. 263 (2012).

13. Phillip Schmandt, *The European Union Model Interoperability Agreement for Electronic Business Documents*, 68 Bus. Law. 271 (2012).

14. Phong Nguyen, *A Survey of Patent Law in Cyberspace*, 68 Bus. Law. 281 (2012).

15. Catherine R. Gellis, *2012 State of the Law Regarding Internet Intermediary Liability for User Generated Content*, 68 Bus. Law. 289 (2012).

16. Cheryl Dancey Balough, *A Survey of False Advertising in Cyberspace*, 68 Bus. Law. 297 (2012).

17. Kristine F. Dorrain & Jonathan T. Rubens, *Trademarks and Copyrights in Cyberspace: A Year in Review*, 68 Bus. Law. 305 (2012).

18. Leland Gardner, *Survey of Domain Name Cases 2011–2012*, 68 Bus. Law. 319 (2012).

"There's No App for That": Calibrating Cybersecurity Safeguards and Disclosures

*By Roland L. Trope**

I. Introduction

No bell tolled when it happened. But the term "cybersecurity" has become an oxymoron like "military intelligence" and "bug-free code." For years the risks of cyber threats remained obscure because companies preferred not to disclose that they had been breached and damaged. The quantum of damages would similarly remain undisclosed, and damages to customers and third parties could not be quantified. Gradually, with data breach reporting statutes taking effect, the realities of quantified financial damages replaced surmise and speculation.[1] During the period reviewed by this survey, April 2011–April 2012, the potential financial costs of a severe breach became clearer as evidenced by the data breach at Sony. The breach of Sony's PlayStation Network resulted in approximately 100 million compromised customer accounts and remediation costs that Sony estimated at $200 million.[2] Sony also faces the added costs of defending the fifty-eight class action suits filed against it based on the breach and any resulting damages if held liable.[3] The year also saw the continued deployment of new communications technologies proceeding far ahead of efforts to assess and mitigate the vulnerabilities that such technologies will introduce to their user communities of companies, customers, and third parties.[4] Illustrative of the trend, U.S. electrical utility companies continued their accelerating deployment of

* Roland Trope is a partner in the New York offices of Trope and Schramm LLP and an Adjunct Professor in the Department of Law at the U.S. Military Academy at West Point. He can be contacted at rltrope@tropelaw.com.

1. For data covering the year in review, see Ponemon Inst. LLC, 2011 Cost of Data Breach Study—United States (2012), *available at* http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide_CODB_US.

2. Nicole Perlroth, *Insurance Against Cyber Attacks Expected to Boom*, N.Y. Times Bits (Dec. 29, 2011, 11:50 AM), http://bits.blogs.nytimes.com/2011/12/23/insurance-against-cyber-attacks-expected-to-boom/.

3. *Id.*

4. U.S. Gov't Accountability Office, Cybersecurity: Threats Impacting the Nation 2, 7–8 (2012) (No. GAO-12-666T), *available at* http://www.gao.gov/assets/600/590367.pdf; Sophos Ltd., Security Threat Report 2012, at 20 (2012), *available at* http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf.

"smart grid" technologies without mitigating the potential cyber risks.[5] As a February 2012 GAO report explained:

> [T]he smart grid vision and its increased reliance on IT systems and networks . . . expose the electric grid to potential and known cybersecurity vulnerabilities . . . . This creates an increased risk to the smooth and reliable operation of the grid. . . . [S]mart grid and related systems have known cyber vulnerabilities. . . . [C]ertain smart meters can be successfully attacked, possibly resulting in disruption to the electricity grid.[6]

An FBI report from May 2010, which became publicly available in April 2012, disclosed that smart meters in Puerto Rico had been hacked to underreport the amount of electricity used by consumers and businesses, causing an estimated annual loss to the utility company of approximately $400 million.[7] A joint security roadmap issued in September 2011 by utilities and their regulators acknowledged that "threats are evolving 'faster than the sector's ability to develop and deploy countermeasures.'"[8]

Counsel advising enterprises faced with such risks will find the emergence of state regulations of smart grid cybersecurity important but limited initially to local significance.[9] In this brief survey of legal developments in 2011–2012, we focus instead on events that will be binding on some enterprises and instructive for counsel in any U.S. jurisdiction when advising clients on the extent to which cybersecurity measures should be reviewed or audited, corrected or enhanced, and the emerging higher standards that such changes may need to meet.

II. *Experi-Metal, Inc. v. Comerica Bank*—Cybersecurity as Measured by "Reasonable Commercial Standards of Fair Dealing"

Whether a financial institution could be held liable for failing to act swiftly and effectively to prevent a cyber-attack from damaging its customers appeared

5. U.S. Dep't of Energy, Audit Report: The Department's Management of the Smart Grid Investment Grant Program 2 (Jan. 2012), (No. OAS-RA-12-04), *available at* http://www.recovery.gov/Accountability/inspectors/Documents/OAS-RA-12-04.pdf.

6. U.S. Gov't Accountability Office, Cybersecurity: Challenges in Securing the Modernized Electricity Grid 11–12 (2012), (No. GAO-12-507T), *available at* http://www.gao.gov/assets/590/588913.pdf.

7. Brian Krebs, *FBI: Smart Meter Hacks Likely to Spread*, KrebsonSecurity.com (Apr. 9, 2010, 10:19 AM), http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/.

8. Joseph Menn, *Power Grid Looks Exposed to Assault*, Fin. Times, Oct. 12, 2011, at 6.

9. At least three states promulgated cybersecurity regulations for utility company deployments of "smart grid" technologies: California, Colorado, and Oklahoma. *See* Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's Own Motion to Actively Guide Policy in California's Development of Smart Grid System, No. 11-07-056 (Cal. P.U.C. July 28, 2011), *available at* http://docs.cpuc.ca.gov/published/FINAL_DECISION/140369.htm; *In re* Proposed Rules Relating to Smart Grid Data Privacy for Electric Utilities, No. 10R-799E (Colo. P.U.C. Aug. 29, 2011), *available at* https://www.dora.state.co.us/pls/efi/efi.show_document?p_dms_document_id=130188&p_session_id=; H.B. 1079, 53d Leg., 1st Sess. (Okla. 2011), *available at* http://webserver1.lsb.state.ok.us/cf/2011-12%20ENR/hB/HB1079%20ENR.DOC.

remote and speculative until the federal district court decision in *Experi-Metal, Inc. v. Comerica Bank*.[10]

Experi-Metal, Inc. ("Experi-Metal"), a custom metal fabricating company incorporated in Michigan, became a customer of Comerica Bank ("Comerica") in September 2000.[11] Three years later, in November 2003, Experi-Metal executed an agreement with Comerica to use Comerica's "Funds Transfer Services" for certain Experi-Metal accounts.[12] Under the parties' written agreement, Experi-Metal could use Comerica's services for wire transfers from two of its accounts (expanded later to include six personal accounts of the company's CEO).[13] A Global Wire Transfer Authorization and Security Procedures document, executed by Experi-Metal in November 2007, authorized Experi-Metal's CEO and its Controller to initiate wire-transfer orders over the telephone once the caller identified him or herself and provided a PIN.[14] Comerica was required to confirm the authenticity of payment orders exceeding $250,000.[15] Experi-Metal did not elect to require a call back to verify the authenticity of a payment order placed by telephone.[16] Later, Experi-Metal removed its Controller from the list of authorized administrative users of Comerica's wire-transfer services.[17]

In April 2008, Comerica notified the administrative users for all online banking accounts of a significant change in its security process: instead of using digital certificates, Comerica would now use "secure token" technology.[18] Each customer administrator received from Comerica a list of active users for their accounts for the previous six months.[19] The list specified each user's ID and a secure token.[20] Comerica asked the customer administrators to notify it if any user ceased to be registered and thus ceased to be authorized to use the online banking services.[21] Although Experi-Metal's list included its Controller (who was no longer authorized), Experi-Metal did not notify Comerica of the error.[22] Instead, Experi-Metal gave one of the secure tokens to its Controller.[23]

On the morning of January 21, 2009, another party alerted Comerica to phishing e-mails sent to Comerica customers by a third party attempting to prompt customers to provide their confidential identification information.[24]

10. No. 09-14890, 2011 WL 2433383 (E.D. Mich. June 13, 2011). For more information on the history of the *Experi-Metal* decision, see Stephen C. Veltri & Greg Cavanagh, *Payments*, 66 BUS. LAW. 1113, 1130–31 (2011).
11. *Comerica Bank*, 2011 WL 2433383, at *2.
12. *Id.*
13. *Id.* at *3.
14. *Id.* at *4–5.
15. *Id.* at *6.
16. *Id.* at *4.
17. *Id.* at *5.
18. *Id.* at *6.
19. *Id.*
20. *Id.*
21. *Id.*
22. *Id.*
23. *Id.*
24. *Id.*

Comerica apparently did not warn its customers.[25] Early the next morning, an Experi-Metal officer received one such phishing e-mail and forwarded it to Experi-Metal's Controller.[26] The Controller clicked on a link within the e-mail (purporting to be a "Comerica Business Connect Customer Form") that sent him to a website.[27] The website asked for his confidential secure token identification, Treasury Management Web ID, and login information, and he witlessly provided it.[28]

Using that information, the third-party adversary started making wire-transfer payment orders from one of the two Experi-Metal accounts authorized for such orders—the Sweep Account.[29] To expand the reach of the fraud, the adversary transferred all of Experi-Metal's General Account Funds to the Sweep Account and did the same with existing and "non-existing" funds from the company's other accounts and the CEO's personal accounts.[30] These "book transfers" totaled more than $5.6 million.[31] Comerica rejected a mere three of the attempted twenty "book transfers," and then only because "[f]unds [were] not available."[32] Most of the funds transferred this way came from Experi-Metal's Employee Savings Account (a zero-balance account into which the company would transfer funds only momentarily before using the funds to pay its employees).[33] These book transfers created a $5 million overdraft in that account.[34]

Between 7:30 a.m. and 2:02 p.m., the adversary executed *ninety-three* fraudulent payment orders totaling over $1.9 million.[35] Most of these payment orders transferred the money to accounts at banks in destinations widely known as sources of cyber-crime (i.e., Russia and Estonia).[36] At approximately 11:30 a.m., J.P. Morgan Chase telephoned Comerica to report six suspicious wire transfers from Experi-Metal's Sweep Account through J.P. Morgan Chase to the accounts of beneficiaries at Alfa-Bank in Moscow, Russia.[37] Twenty minutes later, Comerica contacted Experi-Metal to inquire about the suspicious wire transfers and learned that the company had not authorized any wire-transfer payment orders that day.[38] Within the next half-hour, Comerica had tagged Experi-Metal's accounts so that wire-transfer payment orders would be held up for review before processing. At the same time, Comerica initiated attempts to rescind the previously processed wire-transfer orders.[39] Comerica also disabled Experi-Metal's

25. *Id.*
26. *Id.* at *7.
27. *Id.*
28. *Id.*
29. *Id.*
30. *Id.*
31. *Id.*
32. *Id.*
33. *Id.* at *3, *7.
34. *Id.* at *7.
35. *Id.*
36. *Id.*
37. *Id.*
38. *Id.* at *8.
39. *Id.*

user identifications from the online banking system by changing the passwords and the "'entablement date.'"[40] These actions prevented new access to Experi-Metal's online accounts but did not stop already logged-in users from proceeding with their online activity.[41] As a result, the adversary retained the capability to initiate additional wire-transfer payment orders.[42]

It took Comerica another hour and a half before it could "kill" the adversary's online session at 2:05 p.m.[43] During that period, the adversary initiated fifteen additional fraudulent wire-transfer orders.[44] Comerica eventually cancelled or recovered the funds for all of those fifteen transactions except for one for $49,300.[45] However, during the six-and-a-half hours that the adversary had use of Comerica's wire transfer services and access to Experi-Metal's accounts, it transferred $1.9 million.[46] Comerica eventually recovered approximately $1.4 million, and thus its customers suffered the irrevocable loss of over half a million of its funds.[47] Experi-Metal filed suit seeking to hold Comerica liable for the unrecovered fraudulently transferred funds and alleged that the risk of loss for unauthorized wire transfers fell on Comerica under applicable Michigan statutes.[48]

The district court, after a bench trial, held Comerica liable[49] for reasons that should be of interest to counsel advising clients on the scope of cybersecurity safeguards they should implement. On one hand, the court found that when Comerica accepted the fraudulent wire-transfer orders, which Comerica perceived as coming from and being authorized by Experi-Metal, Comerica adhered to its security procedures.[50] Reading that, counsel might conclude that the bank had done its duty and could not be blamed or held liable. The court, however, reasoned that a bank's compliance with its established, good security procedures was not enough to exonerate a bank from accepting and executing a series of fraudulent wire-transfer orders.[51] The series of orders and the circumstances surrounding them should have aroused suspicions, prompted questions, and led to a hold on processing the transfers until questions into their legitimacy received answers that dispelled any suspicions.[52] At least, that is the thrust of the court's reasoning. The court noted that for Comerica to avoid liability, it had the burden to prove that it acted in "good faith" when it accepted the fraudulent wire-transfer orders as "effective" and originating with Experi-Metal.[53] The measure of "good faith" in this context comes from the definition of

40. *Id.*
41. *Id.*
42. *Id.*
43. *Id.*
44. *Id.* at *9.
45. *Id.*
46. *Id.*
47. *Id.*
48. *Id.* at *1.
49. *Id.* at *1, *14.
50. *Id.* at *11.
51. *Id.* at *24–25.
52. *Id.* at *26.
53. *Id.* at *21.

"good faith" in the Uniform Commercial Code ("U.C.C."), a criterion that cannot be varied by the parties' agreements.[54]

The court explained that "good faith," in Michigan's version of the U.C.C., has a two-pronged definition: "honesty in fact *and* the observance of reasonable commercial standards of fair dealing."[55] Since there was no evidence that "Comerica's employees acted dishonestly in accepting the fraudulent wire transfer orders," the dispositive issue became whether they acted in "observance of reasonable commercial standards of fair dealing."[56] In the court's view, "if 'reasonable commercial standards of fair dealing' obligated Comerica to respond to the fraudulent wire transfer activity in a particular way and Comerica failed to observe those standards," then Comerica cannot show it acted in good faith by demonstrating that its agreements with its customers relieved it of the obligations to adhere to such standards.[57] The court explained that Comerica needed to make two showings: first, present evidence as to what constituted the reasonable commercial standards of fair dealing applicable to a bank's response to the incident involving Experi-Metal; and second, demonstrate by a preponderance of the evidence that Comerica's employees, in their responses to the adversary's phishing attack, met those fair dealing standards.[58] The court, however, concluded that Comerica failed to meet its burden of proof because the expert testimony for Comerica and other evidence failed to inform the court of "whether a bank engages in fair dealing when it allows overdrafts totaling *$5 million* from a single account that usually has a zero balance, particularly where the ten transactions causing the overdrafts were entered repetitively (many in less than a minute of each other) and during one online session."[59] The court found that a "bank dealing fairly with its customer, under these circumstances, would have detected and/or stopped the fraudulent wire activity earlier."[60] Thus, mere adherence to established security procedures will not suffice when the discernible exploits of a cyber-attack should have alerted the bank's personnel to see that there were things seriously wrong in these transfer orders, so much so that the bank's personnel had a duty to do more than follow procedures and process the orders, and should instead have reacted with suspicion and halted the processing in order to find out what was really happening, and, had they done so, the court implies they would have discovered the orders were fraudulent, halted them, and started the recovery efforts sooner. In short, compliance with established security procedures apparently will not prove a bank dealt fairly with a customer when the bank should have detected activities that, despite compliance with

54. *Id.* at *11.

55. *Id.* The court emphasized in a footnote that: "The Official Comments to the U.C.C. indicate that, except where expressly indicated, the obligation of 'good faith' in all Articles of the U.C.C. is the same" and that therefore "cases interpreting 'good faith' within the context of one provision are instructive in defining the term elsewhere." *Id.* at *11 n.3.

56. *Id.* at *11.

57. *Id.* at *12.

58. *Id.* at *13.

59. *Id.*

60. *Id.* at *14.

procedures, raised conspicuous red flags that a bank has a duty to investigate without delay.[61]

The *Comerica Bank* decision should be significant for financial institutions because the court held a bank liable for failing to detect early and respond swiftly and effectively to cyber-based fraud against one of its customers. The fact that the customer could have required call-back verification of wire-transfer orders placed by phone and that the customer's employee allowed himself to be tricked by the phishing attack did not, in the court's view, shift the burden of proof from the bank to the customer. Moreover, the court appears to have reasoned that the extent of the bank's opportunity to detect and interdict the cyber-fraud, as reflected in the number of fraudulent wire transfers, the manifestly suspicious appearance of the transfers (originating in a zero-balance account and directed to an offshore destination and beneficiaries known for cyber-fraud), and the bank's knowledge of prior and the current phishing attempts, increased the bank's burden of proof that it had acted in accordance with "reasonable commercial standards of fair dealing."[62] For any bank in such circumstances, demonstrating that standard as applicable to the circumstances would be difficult, if not elusive, and demonstrating in addition that its employees met such standards would be a significant challenge. Since each such attack may reflect new and increasingly sophisticated tactics by adversaries, a bank may well find it seriously challenged to demonstrate what would be "reasonable commercial standards of fair dealing" in such circumstances.

Comerica Bank therefore appears to offer as a lesson to financial institutions and their counsel that cyber-security policies and procedures need to focus not only on averting and mitigating the damage that could be done to the enterprise from a cyber-attack but also on early detection, quick intervention, and complete interdiction of cyber-fraud or other cyber exploits that have as their ultimate target and result the property of their customers. *Comerica Bank* suggests that it would be prudent for financial institutions and other enterprises that provide their customers online financial or commercial services to review their cyber-security precautions and consider enhancing them to improve the

61. Although it postdates the period under review, the First Circuit decision in *Patco Construction Company v. People's United Bank* reinforces the view that a bank cannot shift liability to its customers through contracts when the bank's security system flagged a potential breach, but the bank failed to interdict the perpetrators' transaction. 684 F.3d 197 (1st Cir. 2012). As the First Circuit noted, Ocean Bank did not have a security system that under Article 4A qualified as "commercially reasonable" because

> [i]n our view, Ocean Bank did substantially increase the risk of fraud by asking for security answers for every $1 transaction, particularly for customers like Patco which had frequent, regular, and high dollar transfers. Then, when it had warning that such fraud was likely occurring in a given transaction, Ocean Bank neither monitored that transaction nor provided notice to customers before allowing the transaction to be completed. Because it had the capacity to do all of those things, yet failed to do so, we cannot conclude that its security system was commercially reasonable. We emphasize that it was these collective failures taken as a whole, rather than any single failure, which rendered Ocean Bank's security system commercially unreasonable.

Id. at 210–11.

62. *Comerica Bank*, 2011 WL 2433383, at *13.

chances that the precautions could meet the standard set in *Comerica Bank*. Other federal courts may find *Comerica Bank*'s reasoning instructive if faced with cases that present similarly slow detection and slow and initially ineffectual responses to cyber-frauds that threaten to cause their customers significant financial damage.

III. SEC Guidance on Cybersecurity Disclosures

In 2011, SEC Chairman Mary Schapiro asked Commission staff to advise her on "whether additional guidance is needed" on whether certain federal securities laws might require a registrant to make cybersecurity disclosures.[63] Although requiring registrants to make such disclosures might be justified for the purpose of giving investors information they arguably need when making their investment decisions, it might also produce unintended adverse consequences for the registrants. The same information required for compliance with the securities laws could be of even greater benefit and value to cyber-adversaries, providing them with information about a registrant that could be used to identify and target vulnerable registrants; discern loopholes for attack vectors; enhance the sophistication of the attack; and facilitate the design of exploits that cloak themselves better, take longer to detect, prove more resistant to remediation, and, as a result, cause greater damage to targeted registrants, assets, and third parties. The SEC Division of Corporate Finance (the "Staff") recognized these risks and highlighted them in the cybersecurity guidance the Staff issued on October 13, 2011 (the "Guidance").[64]

The Staff attempted to strike a balance in the Guidance between requiring a registrant to disclose information needed by investors and relieving registrants of any obligation to make disclosures that would assist cyber-adversaries in attacking the registrant. The Staff highlighted the oft-reported trend of enterprises, including registrants, that have "migrated toward increasing dependence on digital technologies to conduct their operations"[65] and stated that such dependence has come at a high, belatedly recognized price as "the risks to registrants associated with cybersecurity have also increased, resulting in more frequent and severe cyber incidents,"[66] many of which include "gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption."[67] The Staff noted that the "objectives of cyber attacks vary widely and may include theft of financial assets, intellectual property, or other sensitive information belonging to

63. Roland L. Trope & Sarah Jane Hughes, *The SEC Staff's "Cybersecurity Disclosure" Guidance: Will It Help Investors or Cyber-thieves More?*, Bus. L. Today, Dec. 2011, at 1, *available at* http://apps.americanbar.org/buslaw/blt/content/2011/12/article-3-trope-hughes.pdf.

64. Div. of Corp. Fin., U.S. Sec. & Exch. Comm'n, CF Disclosure Guidance: Topic No. 2—Cybersecurity (Oct. 13, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

65. *Id.*

66. *Id.*

67. *Id.*

registrants, their customers, or other business partners."[68] Moreover, the Staff emphasized that victims of cyber attacks may suffer multiple and substantial costs:

- Remediation costs . . . for stolen assets . . . and repairing system damage . . . [and] incentives offered to customers or other business partners in an effort to maintain the business relationships after an attack;
- Increased cybersecurity protection costs . . . ;
- Lost revenues resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- Litigation; and
- Reputational damage adversely affecting customer or investor confidence.[69]

However, note that each of those costs would likely increase if a registrant made timely and informative disclosures concerning the condition of its cybersecurity and its experience of cyber attacks, which probably explains why registrants and other enterprises have been reluctant to release such information to the public (and why few registrants, to date, have made cybersecurity disclosures).[70]

Consider what the Guidance requires registrants to disclose and the point at which it relieves them of that obligation. The Guidance informs registrants that

68. *Id.*

69. *Id.*

70. Although some registrants, such as Google, Intel, and ConEdison, have made limited cybersecurity disclosures, some registrants, such as Lockheed Martin, have apparently decided to postpone or avoid such disclosures despite public reports of having experienced severely damaging cyber attacks in 2011. For example, ConEdison's forward-looking statements in its 10Q for the filing period September 30, 2011 include the following statement: "Actual results or developments might differ materially from those included in the forward-looking statements because of various risks, including . . . a cyber attack could adversely affect the Companies." Moreover, under Item 1A, Risk Factors, of its 10Q for the quarterly period ended September 30, 2011, ConEd stated the following:

> **A Cyber Attack Could Adversely Affect the Companies.** The Utilities and other operators of critical energy infrastructure may face a heightened risk of cyber attack. In the event of such an attack, the Utilities and the competitive energy businesses could have their operations disrupted, property damaged and customer information stolen; experience substantial loss of revenues, response costs and other financial loss; and be subject to increased regulation, litigation and damage to their reputation.

Consolidated Edison., Inc. & Consolidated Edison Co. of N.Y., Inc., Quarterly Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the Quarterly Period Ended Sept. 30, 2011 (Form 10-Q), at 5, 61 (Nov. 3, 2011). Curiously, ConEd's 10Q for the period ending March 31, 2012 only contains the bare-bones statement that "[a] cyber attack could adversely affect the Companies" and omits the detailed statement it disclosed in the Risk Factors for the third quarter 2011 10Q. *See* Consolidated Edison, Inc. & Consolidated Edison Co. of N.Y., Inc., Quarterly Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the Quarterly Period Ended Mar. 31, 2012 (Form 10-Q), at 5, 51 (May 3, 2012).

they should reveal the following kinds of information, each of which will arguably be better understood and of more significance and value to an adversary (before and after an attack on the registrant) than to an investor (before and after making an investment in the registrant):

- "[D]isclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky."[71]
- Discuss "aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences."[72]
- Describe the extent to which the "registrant outsources functions that have material cybersecurity risks" and "how the registrant addresses those risks."[73]
- Describe the registrant's experience of cyber incidents that are "individually, or in the aggregate, material, including a description of the costs and other consequences."[74]
- Describe "relevant insurance coverage"[75] and, rather incredibly, in view of the exposure such disclosure would cause the registrant.
- Describe risks "related to cyber incidents that may remain undetected for an extended period."[76]

The Guidance seeks to limit the risks it thereby encourages registrants to make by acknowledging that "[w]e are mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts—for example, by providing a 'roadmap' for those who seek to infiltrate a registrant's network security."[77] The Guidance emphasizes that "disclosures of that nature are not required under the federal securities laws."[78] Of course, without knowing what exploits an adversary plans, or the intelligence an adversary has gathered on a targeted registrant's digital assets and vulnerabilities, few, if any, registrants and counsel could meaningfully and accurately assess whether a cybersecurity disclosure would provide an adversary a "roadmap" (a vague standard that invites conflicting interpretations, e.g., the Staff might interpret the term "roadmap" as denoting a comprehensive map, but a registrant's counsel might reasonably interpret "roadmap" to mean any data that would facilitate an attack). To avoid such conflicts and the risk they pose to a registrant client, its counsel could reasonably

71. DIV. OF CORP. FIN., U.S. SEC. & EXCH. COMM'N, CF DISCLOSURE GUIDANCE: TOPIC NO. 2—CYBERSECURITY (Oct. 13, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
72. *Id.*
73. *Id.*
74. *Id.*
75. *Id.*
76. *Id.*
77. *Id.*
78. *Id.*

interpret the Guidance to provide a bright-line test, namely that if the disclosure would "compromise cybersecurity efforts,"[79] then the federal securities laws do not require it, or relieve the registrant of what otherwise might be a duty to disclose it.

The Guidance's own examples illustrate the tension between an apparently required cybersecurity disclosure and an apparent relief of that requirement. The Guidance notes that in the event that a registrant experiences the theft of "material intellectual property" by cyber attack and if the "effects of the theft are reasonably likely to be material," then the registrant should publicly disclose a description of the stolen property and "the effect of the attack on its results of operations, liquidity, and financial condition and whether the attack would cause reported financial information not to be indicative of future operating results or financial condition."[80] True, such information may be material for an investor considering the purchase or sale of a registrant's securities. However, such information may also compromise the registrant's cybersecurity efforts to an extent that the registrant and its counsel can only know by speculation and inferences drawn from surmises and assumptions. A cyber adversary, for example, may misappropriate thousands of files from a registrant without knowing the value of their contents, until informed by a registrant's disclosure that such files included "material intellectual property," the theft of which could have a serious effect on the financial condition of the registrant. Armed with such inside information, the adversary may now have a market for the files that it might otherwise have failed to appreciate, and the sale of those files may compound the compromise of the registrant's cybersecurity efforts.

Similarly, the Guidance advises that "if a registrant has a new product in development and learns of a cyber incident that could materially impair its future viability, the registrant should discuss the incident and the potential impact to the extent material."[81] Here again, the disclosure could reveal to the cyber thieves which of the stolen properties holds value, whether in re-sale or as the basis for a ransom demand to the registrant. These examples also demonstrate that the disclosure is at least as likely, if not more likely, to be of immediate and significant value for the adversaries (past and future) than for the investor community. The few cybersecurity disclosures that have been made in the months since the Staff issued the Guidance suggest that registrant's counsel has recognized that the risks of disclosure outweigh the risks of noncompliance, and that, if so, registrant's counsel can justify withholding or significantly postponing such disclosures on the grounds offered by the Guidance where it states the following: "[W]e reiterate that the federal securities laws do not require disclosure that itself would compromise a registrant's cybersecurity. Instead, registrants should provide sufficient disclosure to allow investors to appreciate the

79. *Id.*
80. *Id.*
81. *Id.*

nature of the risks faced by the particular registrant in a manner that would not have that consequence."[82]

Regrettably, the Staff does not appear to have recognized (or has decided not to acknowledge) that a registrant's best protection of its cybersecurity is to withhold any information that could compromise its cybersecurity—or postpone it to a time when its defenses have been shored up and the value of the information to an attacker has been neutralized. Moreover, registrant's counsel will want to remain sensitive to the overriding fact of the current typography of cyber threats: the attacker need only find one gap, one loophole, in the target's defenses in order to gain access often to the target's entire network; but, by contrast, a target must find and close every gap and loophole in order to achieve reliable and resilient cybersecurity. That asymmetry between attacker and target puts the target at such a disadvantage that it severely limits the possible good that the Guidance can achieve for the investor community and makes the disclosures it seeks to encourage a dubious risk for any registrant to take. Counsel may prefer the caution of a minimally compliant disclosure in its SEC filings and decide to wait for the SEC Staff to ask for more, rather than to risk providing intelligence that could aid an adversary planning or continuing a cyber attack.[83]

IV. Conclusion

The period 2011–2012 saw cyber attacks become more widespread, severe, and financially damaging. The legal developments have increased the stress on an enterprise's officers and directors and their counsel. Cybersecurity can no longer be focused exclusively on protecting the enterprise and its assets and reputation, but, in light of *Comerica Bank*, cybersecurity measures need to be broadened if an enterprise is to be in a position to defend its response to a cyber attack. The longer it takes an enterprise to detect an attack that results in damage to a customer or a third party with whom the enterprise has a formal commercial or corporate relationship, and the longer it takes the enterprise in such circumstances to interdict and remediate the attack, the harder pressed the enterprise and its counsel will be to demonstrate to a court that the enter-

82. *Id.*

83. To date, it appears that most registrants have interpreted the Guidance so narrowly as to avoid having to make a disclosure. As was recently observed:

> Hackers broke into computers at hotel giant Wyndham Worldwide Corp. three times in two years and stole credit card information belonging to hundreds of thousands of customers. Wyndham didn't report the break-in in corporate filings even though the Securities and Exchange Commission wants companies to inform investors of cybercrimes.
>
> Amid whispers of sensational online break-ins resulting in millions of dollars in losses, it remains remarkably difficult to identify corporate victims of cybercrimes. Companies are afraid that going public would damage their reputations, sink stock prices or spark lawsuits.

Cybercrime Disclosures Rare Despite New SEC Rule, NPR.ORG (June 29, 2012), http://www.npr.org/templates/story/story.php?storyId=155965721.

prise's actions did not fall short of "reasonably commercial standards of fair dealing."[84] If the targeted enterprise (and the damaged customers or other third parties) are registrants, then such registrants and their legal counsel will need to consider what, if any, cybersecurity disclosure the registrant may need to make to comply with the Guidance. To do so, they may also need to consider what will be the Staff's interpretations of what disclosures and nondisclosures related to the security incident would be consistent with the requirements of the applicable federal securities laws and regulations for risk factor disclosures, management's discussion and analysis of financial condition results of operations, description of business, legal proceedings, and financial statement disclosures. Although the Guidance takes the view that somewhere short of providing a "roadmap" to attack a targeted enterprise there should be information of value to the investor community, it remains far from certain whether experienced counsel can prudently advise a registrant client to take such a risk, particularly when counsel cannot possibly know an adversary's plans and capabilities, its intelligence of the client's vulnerabilities, and what advantage may be transferred to an adversary by a seemingly well-scrubbed disclosure. In the forthcoming years, these kinds of judgment calls may pose increasingly serious challenges to an enterprise's counsel.

84. See, for example, the interpretation of *Comerica Bank* and *Patco Construction* offered in a recent article:

> Banks typically are responsible for losses when personal accounts are hacked. But state laws uniformly place the burden on commercial clients to show that banks didn't do enough to protect their money. The laws generally have treated individuals and companies differently, reasoning that companies should be more sophisticated than individuals and have their own online security measures in place. The two recent rulings [*Comercia Bank* and *Patco Construction*] may alter that equation, recognizing small business owners often lack an understanding of cyberthreats when they accept bank security procedures, said lawyers who represent owners in such disputes.

Joe Palazzolo, *Cyberthieves Hit Owners: Courts Extend Legal Protection to Small Firms Whose Accounts Were Hacked*, Wall St. J., July 19, 2012, at B7.

Developments in the Law Concerning Geolocational Privacy

*By Theodore F. Claypoole and Richard C. Balough**

The law of geolocational privacy evolved in the past year in case law, in a new rule at the Federal Trade Commission, and in proposed federal legislation. The law of geolocational privacy arises from the use of tracking or locating technology to pinpoint more accurately the physical location of a person. Generally this tracking is performed using a mobile device or a beacon with global positioning system ("GPS") capability.[1] Smartphones offer several methods of tracking their holders, including GPS, triangulation of cell towers, and wi-fi pickups, and law enforcement regularly requests both real-time and historical information related to a cell phone's location from phone companies without a warrant.[2] Many cars have tracking technology from a manufacturer or insurance company. Cameras at intersections and buildings can be used for geolocational tracking because they show the time that a certain person entered the camera's view, and security cards and toll booth fast passes clock a time and location.

I. GPS Tracking

The most anticipated recent case concerning geolocational privacy involved a criminal conviction based on GPS technology. In *United States v. Jones*,[3] the U.S. Supreme Court had the opportunity to address whether nearly constant

* Theodore F. Claypoole is a member of the firm of Womble Carlyle Sandridge & Rice in Charlotte, North Carolina. He is the senior member of the firm's Intellectual Property Practice Group. Richard C. Balough is a member of Balough Law Offices, LLC in Chicago, Illinois, practicing in the area of intellectual property. Mr. Claypoole and Mr. Balough are co-chairs of the Mobile Commerce Subcommittee of the Cyberspace Law Committee of the Section of Business Law.

1. *Geolocational Privacy and Surveillance Act: Hearing on H.R. 2168 Before the H. Subcomm. on Crime, Terrorism & Homeland Security*, 112th Cong. (2012) (statement of Marc Rotenberg, President, Electronic Privacy Information Center), *available at* http://epic.org/privacy/location_privacy/EPIC-Location-Privacy-Statement-5-17-12.pdf.

2. David H. Goetz, *Locating Location Privacy*, 26 Berkeley Tech. L.J. 823, 824 (2011) (citing *In re* Application of the U.S. for an Order for Disclosure of Telecomm. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005) (holding that warrantless access to cell site location information by the government is not a violation of the Fourth Amendment)); *but see In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 840 (S.D. Tex. 2010) (holding that warrantless access by the government to cell site location information is a violation of the Fourth Amendment).

3. 132 S. Ct. 945 (2012).

monitoring of a person's location was a violation of the person's expectation of privacy; however, it decided the case on a narrower ground, leaving for another day a full review of the issue of geolocational privacy.[4] In *Jones*, a drug dealer was convicted based in part on information obtained when a GPS tracking device was placed on his car without a warrant.[5] The device reported the suspect's location every ten seconds for twenty-eight days.[6] The appellate court threw out the conviction, finding that use of the GPS tracking device for such a lengthy period of time required a warrant.[7] It held that, while a person has no expectation of privacy on a public thoroughfare, a "reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there. Rather, he expects each of these movements to remain 'disconnected and anonymous.' "[8]

Reflecting the reasoning in *DOJ v. Reporters Committee for Freedom of the Press*,[9] the appellate court stated that

> [a] person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[10]

This holding was contradicted by *United States v. Cuevas-Perez*,[11] where the defendant's car was tracked for sixty hours during a road trip through New Mexico, Texas, Oklahoma, Missouri, and finally Illinois, when the GPS battery gave out, requiring the Immigration and Customs Enforcement agents to ask that the Illinois police follow his car and pull him over for any type of violation, which the police did.[12] The divided *Cuevas-Perez* court said *Maynard* "is wrongly decided."[13]

In *Jones*, the Supreme Court agreed that surreptitiously placing a tracking device on a suspect's car and electronically tracking the car wherever it went could not be conducted without a judicial warrant.[14] However, the justices disagreed as to whether the police's actions intruded on the suspect's reasonable expectation of privacy as described in *Katz v. United States*.[15] A five-member majority held that the police trespassed on the suspect's car when placing the tracking

4. *Id.* at 954.
5. A warrant had expired before the GPS device was placed on the vehicle. *Id.* at 948.
6. *Id.*
7. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010). Maynard was a co-defendant who did not participate in the appeal to the Supreme Court.
8. *Id.* at 563.
9. 489 U.S. 749 (1989).
10. *Maynard*, 615 F.3d at 561–62.
11. 640 F.3d 272 (7th Cir. 2011), *vacated*, 132 S. Ct. 945 (2012). The case was remanded to the United States Court of Appeals for the Seventh Circuit for further consideration in light of United States v. Jones, 132 S. Ct. 945 (2012).
12. *Cuevas-Perez*, 640 F.3d at 273.
13. *Id.* at 276.
14. United States v. Jones, 132 S. Ct. 945, 964 (2012).
15. 389 U.S. 347 (1967).

device there.[16] That trespass required a warrant because the Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures," and the suspect's car was an "effect" protected against unwarranted trespass by the government.[17] The majority held that the trespass made it unnecessary to answer the question of whether the *Katz* "reasonable expectation of privacy" test was met.[18] Justice Scalia stated, "We may have to grapple with these 'vexing problems' in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here."[19]

Four members of the *Jones* Court concurred in the judgment but accused the majority of shirking its responsibility to address the truly "vexing problems" of the *Jones* case, including whether the simple act of electronically monitoring a suspect for twenty-eight days without a warrant is allowed under the Fourth Amendment. The primary concurrence, written by Justice Alito, chided the majority for relying on "18th-Century Tort Law" that "has little if any support in current Fourth Amendment case law [and] . . . is highly artificial."[20] The four-judge minority felt that the *Jones* case should have been decided against the government because the tracked suspect had a reasonable expectation that his movements would not be electronically monitored every ten seconds for four straight weeks.[21]

Justice Sotomayor, who joined the majority opinion, also wrote a concurrence in which she agreed with Justice Alito "that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.' "[22] She wrote that awareness that the government may be watching "chills associational and expressive freedoms."[23] Justice Sotomayor observed that, while

> it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties[,] [t]his approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks [such as texting, the URLs that they visit, and the e-mail addresses to which they correspond].[24]

The concurrence written by Justice Alito similarly noted that in the pre-computer age, the

> greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly

16. *Jones*, 132 S. Ct. at 951.
17. *Id.* at 949.
18. *Id.* at 954.
19. *Id.*
20. *Id.* at 958 (Alito, J., concurring).
21. *Id.*; *see also* State v. Zahn, 812 N.W.2d 490, 499 (S.D. 2012) (concluding that the attachment and use of a GPS device to monitor an individual's activities over an extended period of time requires a warrant because "the unfettered use of surveillance technology could fundamentally alter the relationship between our government and its citizens").
22. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).
23. *Id.* at 956.
24. *Id.* at 957 (citation omitted).

> and therefore rarely undertaken. . . . Devices like the one used in this present case, however, make long-term monitoring relatively easy and cheap. In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.[25]

In *United States v. Arrendondo*, decided after *Jones*, the district court denied a motion to suppress evidence gathered pursuant to a warrant using a GPS tracking device that was installed in a package.[26] Ultimately, the GPS device tracked the defendant's package while it was in a truck that was moving in public places.[27] The court reasoned that there was no Fourth Amendment violation because, unlike the *Jones* case, "no law enforcement officer trespassed on defendant's vehicle to install a tracking device" because the package was placed in the truck by the defendant.[28]

II. Cases Involving Cell Phone Information

In other geolocational tracking cases prior to *Jones*, courts questioned the extent of a person's expectation of privacy for records that identify and triangulate the base station towers for cell phones. With such information, the government can determine a person's exact location when placing calls, e-mailing, or texting.[29] Pursuant to section 201 of the Electronic Communications Privacy Act of 1986, the government may demand disclosure of records pertaining to a subscriber only with a court order, which "shall issue only if the government entity offers specific and articulable facts showing that there are reasonable grounds to believe" that the communication is relevant to an ongoing criminal investigation.[30] This showing is lower than the probable cause required for a warrant.

In *United States v. Graham*,[31] the issue was the suppression of historical data for cell site location records obtained pursuant to the Stored Communications Act. The data was grouped in two sets. The first was for fourteen days and 1,628 individual cell site locations.[32] The second set was for 221 days and 20,235 cell site locations.[33] The court found that "historical cell site location records are records created and kept by third parties that are voluntarily conveyed to those third parties by their customers."[34] As such, there was no expectation of privacy because the information was "voluntarily conveyed" by the defendants to a third party.[35] The district court distinguished the facts from *Jones* by noting that *Jones*

25. *Id.* at 963–64 (Alito, J., concurring).
26. No. 11-cr-63-FtM-29DNF, 2012 U.S. Dist. LEXIS 66919, at *3 (M.D. Fla. May 14, 2012).
27. *Id.* at *5–6.
28. *Id.* at *18; *but see* United States v. Katzin, No. 11-226, 2012 U.S. Dist. LEXIS 65677, at *36 (E.D. Pa. May 9, 2012) (granting defendant's motion to suppress evidence gathered using a GPS device attached to a car without a warrant and tracking the vehicle on a public road).
29. *Jones*, 132 S. Ct. at 963 (Alito, J., concurring).
30. 18 U.S.C. § 2703(d) (2006).
31. No. 11-0094, 2012 U.S. Dist. LEXIS 26954 (D. Md. Mar. 1, 2012).
32. *Id.* at *7.
33. *Id.*
34. *Id.* at *48.
35. *Id.* at *56.

> concerned the prolonged surveillance of a vehicle by global positioning system technology, and not through historical cell site location data. That distinction is important. Historical cell site location data is, as its name implies, historical—the information revealed by such data exposes to the government only where a suspect *was* and not where he is. The GPS technology at issue in *Maynard*, on the other hand, revealed to the government the location and movements of the suspect in real time. . . . The GPS data in *Maynard* provided coordinates of the suspect's vehicle for the government to collect and analyze. Here, by contrast, the historical cell site location records provided to the government by the Defendants' cellular providers only reveal which cellular towers were used to route a particular call.[36]

The district court, after analyzing the opinions in *Jones*, found that the Supreme Court did not "definitively conclude that an aggregation of surveillance records infringes a Fourth Amendment legitimate expectation of privacy."[37] The district court further relied on the statements in *Jones* that there is no legitimate expectation of privacy in information voluntarily turned over to third parties.[38]

In contrast, in *In re United States for an Order Authorizing the Release of Historical Cell-Site Information*,[39] a district court in New York denied the government's request for cell tower information. The court noted that "cell-site-location records present even greater constitutional concerns than the tracking at issue in *Maynard*."[40] It found that cell-site location records enable the tracking of the vast majority of Americans: "Thus, the collection of cell-site-location records effectively enables 'mass' or 'wholesale' electronic surveillance, and raises greater Fourth Amendment concerns than a single electronically surveilled car trip."[41] The court rejected the argument that a cellphone user voluntarily discloses his location by turning on his phone and making and receiving calls and texts.

The issue of the use of cell phones to determine a person's location also has arisen outside the criminal courts. In *Cousineau v. Microsoft Corp.*,[42] the plaintiff seeks class action status in a complaint against Microsoft, alleging that even after a user clicked to deny Microsoft access to her geolocation, Microsoft continued to collect the information.[43] "Thus, Microsoft surreptitiously forced even unwilling users into its non-stop geo-tracking program in the interest of developing its digital marketing grid."[44] As of June 2012, the case was in the discovery phase.

36. *Id.* at *19–20 (citation omitted).
37. *Id.* at *30.
38. *Id.* at *56.
39. 809 F. Supp. 2d 113 (E.D.N.Y. 2011).
40. *Id.* at 119.
41. *Id.* at 118; *but see Graham*, 2012 U.S. Dist. LEXIS 26954, at *65 ("Even if the government's acquisition of historical cell site location records in this case had been in violation of the Defendants' *Fourth Amendment* rights, it obtained those records in good faith reliance on a constitutional statute and valid Orders . . . .").
42. No. 11-cv-01438-JCC (W.D. Wash. filed Aug. 21, 2011).
43. Amended Class Action Complaint at 3, Cousineau v. Microsoft Corp., No. 11-cv-01438-JCC (W.D. Wash. Oct. 17, 2011).
44. *Id.*

III. Cases Alleging Breach of Contract or Consumer Protection Laws

Another approach to addressing geolocational privacy involves suing mobile device manufacturers for breaching promises or for violating consumer protection laws. In *Goodman v. HTC America, Inc.*,[45] the plaintiffs alleged that a mobile phone manufacturer and application developer installed a local weather application ostensibly to provide convenient weather reports, but they subsequently used the application to transmit the plaintiffs' locations for other purposes, including for "fine" geographic location data, which identifies the latitude and longitude of a particular device's location within several feet at a given date and time.[46] The defendants have filed a motion to dismiss arguing, among other things, that the plaintiffs failed to allege any injury.[47]

In *In re iPhone/iPad Application Consumer Privacy Litigation*,[48] various plaintiffs sought class action certification for a case against Apple Inc. and other tracking defendants[49] alleging, among other things, that the defendants, without the plaintiffs' knowledge, collected precise home and workplace locations and "current whereabouts" of the plaintiffs by using certain features of iPhone and iPad operating systems and applications.[50] The district court granted motions to dismiss the complaint with leave to amend on the ground that the plaintiffs failed to allege sufficient facts to establish the court's Article III standing.[51] The court noted it "does not take lightly Plaintiffs' allegations of privacy violations" but that, "[d]espite a lengthy Consolidated Complaint, Plaintiffs do not allege injury in fact to *themselves*."[52] The plaintiffs filed their amended complaint,[53] and the defendants filed a new motion to dismiss.[54] The court granted the other tracking defendants' motion to dismiss along with all counts against Apple relating to the Stored Communications Act, the Wiretap Act, the Computer Fraud and Abuse Act, and the California Constitution.[55] The court allowed only two counts against Apple to proceed, but those counts concern misrepresentations rather than a right of privacy regarding geolocation.[56]

45. No. 11-cv-01793-MJP (W.D. Wash. filed Oct. 17, 2011).

46. First Amended Supplemented Complaint—Class Action at 1–2, Goodman v. HTC Am., Inc., No. 11-cv-01793-MJP (W.D. Wash. Feb. 10, 2012).

47. Reply in Support of Accuweather Defendants' Motion to Dismiss Second Amended Supplemented Complaint—Class Action at 2–8, Goodman v. HTC Am., Inc., No. 11-cv-01793-MJP (W.D. Wash. May 2, 2012).

48. No. 11-MD-2250-LHK (N.D. Cal. filed Aug. 25, 2011).

49. Flurry, Inc.; Mobclix; Pinch Media, Inc.; Trafficmarketplace.com, Inc.; Mellenial Media; AdMarvel, Inc.; Google, Inc.; AdMob, Inc.; and Medialets, Inc.

50. First Amended Consolidated Class Action Complaint at 2, 4, 6, *In re* iPhone/iPad Application Consumer Privacy Litig., No. 11-MD-2250-LHK (N.D. Cal. Nov. 22, 2011).

51. Order Granting Defendants' Motions to Dismiss at 1, *In re* iPhone/iPad Application Consumer Privacy Litig., No. 11-MD-2250-LHK (N.D. Cal. Sept. 20, 2011).

52. *Id.* at 6.

53. The First Amended Consolidated Class Action Complaint was filed on November 22, 2011.

54. The Motion to Dismiss was filed on January 10, 2012.

55. Order Granting in Part and Denying in Part Defendants' Motion to Dismiss at 1, *In re* iPhone/iPad Application Consumer Privacy Litig., No. 11-MD-2250-LHK, slip op. at 1 (N.D. Cal. June 12, 2012) (order granting in part and denying in part defendants' motion to dismiss).

56. *Id.* at 2.

IV. Federal Trade Commission Changes to COPPA Rules

In fall 2011, the Federal Trade Commission sought comments on amendments to the Children's Online Privacy Protection Act ("COPPA") rules.[57] COPPA generally limits the type of information that online service providers that direct their activities toward children may collect for children under thirteen.[58] The existing COPPA rules prohibit the collection of personal information from children, including addresses.[59] The revision to the rule adds a new section to the definition of "personal information" to include "[g]eolocation information sufficient to identify street name and name of a city or town."[60] In the comments proposing the rule, the FTC said in its view "geolocation data that provides information at least equivalent to 'physical address' should be covered as personal information."[61] On August 6, 2012, the FTC issued a supplemental notice for proposed rulemaking to refine further the definition of personal information.[62]

V. Proposed Federal Geolocational and Privacy Surveillance Act

Pending before Congress is the Geolocational Privacy and Surveillance Act. The Act would prohibit "any Person" from intentionally intercepting or disclosing location data and the use of location information by any person "knowing or having reason to know that the information was obtained through the interception of such information" in violation of the Act.[63] The Act defines "geolocation information" as

> any information that is not the content of a communication, concerning the location of a wireless communication device or tracking device . . . that, in whole or in part, is generated by or derived from the operation of that device and that could be used to determine or infer information regarding the location of the person.[64]

The Act allows for intercepting geolocation information that is gathered in the normal course of business, for conducting foreign surveillance, when the person or the parent or guardian of a child has given prior consent, in an emergency, or where a law enforcement official has obtained a warrant.[65] The Act provides that an individual whose geolocation information is intercepted, disclosed, or intentionally used in violation of the Act may obtain actual and punitive damages, or

57. Children's Online Privacy Protection Rule, 76 Fed. Reg. 59804 (proposed Sept. 27, 2011) (to be codified at 16 C.F.R. pt. 312).
58. Children's Online Privacy Policy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2006).
59. 16 C.F.R. § 312.2(b) (2012).
60. Children's Online Privacy Protection Rule, 76 Fed. Reg. at 59830 (modifying 16 C.F.R. § 312.2(j)).
61. *Id.* at 59813.
62. Children's Online Privacy Protection Rule, 77 Fed. Reg. 46643 (proposed Aug. 6, 2012) (to be codified at 16 C.F.R. pt. 312).
63. Geolocational Privacy and Surveillance Act, H.R. 2168, 112th Cong. § 2602(a)(1)(A)–(B) (2012).
64. *Id.* § 2601(3).
65. *Id.* § 2602(b)–(h).

statutory damages of $100 per day or $10,000 total.[66] The House and Senate have conducted hearings, but no final vote has been taken.

VI. Conclusion

It is likely that during the coming year, there will be more attention paid to geolocational privacy, both in court cases and through legislation. While the *Jones* case tangentially discussed geolocation as it relates to the Fourth Amendment, the decision did not address the fundamental question of whether there is a reasonable expectation of privacy when prolonged GPS monitoring is involved. Some private plaintiffs still are pursuing whether it is a reasonable expectation for individuals to have locational privacy when using smart devices. Finally, it is expected that at least some members of Congress will continue to push for legislation that protects some aspects of geolocational privacy.

66. *Id.* § 2605(b)(2), (c)(1)–(2).

Survey of Recent European Union Privacy Developments

*By W. Gregory Voss**

I. Introduction

During the past year, the European Union ("EU") witnessed important privacy developments. Certain of these developments, including a preliminary ruling on Spain's implementing legislation that added a condition to the processing of personal data, guidance on facial recognition and biometric technologies, and the meaning of consent, are discussed below. Other developments related to cookies, which are principally dealt with by telecommunications legislation rather than pure data privacy legislation, are addressed elsewhere in this year's Survey of Cyberspace Law.[1]

Proposals for new, more robust legislation at the EU level, which are briefly treated here, may lead to the replacement of the existing EU data protection framework[2]—already described as putting "stringent standards on the collection of electronic data by the government and by any other entity."[3] In this globalized world where information frequently travels across borders, the potential adoption of the proposed EU data protection legislation is of great importance to legal practitioners on both sides of the Atlantic.

II. Developments Under the Present System

A. Spanish Legislation

On November 24, 2011, the Court of Justice of the European Union ("ECJ") rendered its decision in two proceedings[4] that were referred to it for a preliminary

* Toulouse University, Toulouse Business School; Member of the Institut de Recherche en Droit Européen International et Comparé (IRDEIC), Toulouse, France.

1. *See* Robert Bond, *The EU E-Privacy Directive and Consent to Cookies*, 68 Bus. Law. 215 (2012).

2. *See* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) [hereinafter Directive].

3. William R. Denny, *Survey of Recent Developments in the Law of Cloud Computing and Software as a Service Agreement*, 66 Bus. Law. 237, 239 (2010). For a more extensive discussion of the Directive, see Ariane Siegel et al., *Survey of Privacy Law Developments in 2009: United States, Canada, and the European Union*, 65 Bus. Law. 285, 299–305 (2009).

4. Joined Cases, Case C-468/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) v. Administración del Estado, [2012] 1 C.M.L.R. 48 (Nov. 24, 2011); Case C-469/10, Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, [2012] 1 C.M.L.R. 48 (Nov. 24, 2011).

ruling by the Spanish *Tribunal Supremo* ("Spanish Supreme Court") on September 28, 2010. The two proceedings, one between the National Association of Credit Institutions ("ASNEF") and the Spanish State Administration, and the other between the Federation of Electronic Commerce and Direct Marketing ("FECEMD") and the Spanish State Administration, had been joined by the ECJ and involve an interpretation of Council Directive 95/46 ("Directive").[5]

In the joined cases involving ASNEF and FECEMD, the ECJ considered whether Spain had correctly implemented Article 7 of the Directive or whether in implementing Article 7 it had exceeded the limits of the Directive. Article 7 of the Directive provides that:

> Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or . . . (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).[6]

The Spanish legislation implementing the Directive added a condition to the processing of personal data in its Article 6(2), which is otherwise similar to Article 7(f) of the Directive, that data be in sources available to the public.[7] ASNEF and FECEMD each made administrative challenges to certain articles of the Spanish Royal Decree that was used to implement the Spanish legislation, on the ground that this condition to legitimate personal data processing, which did not exist in the Directive, had been added.[8]

The ECJ ruled that this national legislation, which adds the requirement that "the data should appear in public sources," is precluded by Article 7(f) of the Directive, which has direct effect.[9] Thus, litigants have grounds for challenging national laws that "impose additional requirements that have the effect of amending the scope of one of the six principles provided for in [Article] 7."[10] Article 7(f) "may be relied on before the national courts by individuals against the State where the latter has . . . failed to implement that directive correctly,"[11] as was the case with the challenges by ASNEF and FECEMD.

In its discussion of one of the questions referred to it, the court cited by analogy *Productores de Música de España (Promusicae) v. Telefónica de España SAU* for the proposition that in the transposition of the Directive member states must "take care to rely on an interpretation of [the Directive] which allows a fair balance to be struck between the various fundamental rights and freedoms pro-

5. *Id.* ¶ 2.
6. *Id.* ¶ 6 (quoting Directive, *supra* note 2, art. 7(a), (f)). The "controller" is the party that "determines the purposes and means of the processing of personal data." Directive, *supra* note 2, art. 2(d) (defining "controller").
7. Organic Law 15/1999 on the Protection of Personal Data art. 6(2) (B.O.E. 1999, 298) (Spain); *ASNEF*, [2012] 1 C.M.L.R. 48, ¶ 10.
8. *ASNEF*, [2012] 1 C.M.L.R. 48, ¶¶ 15–17.
9. *Id.* ¶ 49.
10. *Id.* ¶ 32.
11. *Id.* ¶ 51.

tected by the EU legal order,"[12] but then the court emphasized that such balancing should be done on a case-by-case basis, and not in a "categorical and generalised"[13] manner, such as through the adoption of the challenged provisions of the Spanish national legislation.[14] As a result of this case, on February 8, 2012, the Spanish Supreme Court annulled part of the Spanish Royal Decree used to implement the Spanish legislation.[15]

Thus, harmonization of EU member state laws, generally a goal of directives, will be enhanced as a result of this decision relating to privacy. Harmonization, although not considered adequate today in the area of EU privacy law (as discussed in Part III.A. below), gives businesses some degree of comfort that they will be treated similarly when operating in different EU member states. Furthermore, this case also brings focus on the limited and exhaustive list of legitimate reasons for the processing of personal data contained in Article 7 of the Directive, as well as the necessity for firms subject to the provisions of the Directive to fit within one of those legitimate reasons, such as by obtaining unambiguous consent (as discussed in Part II.B.1. below).

B. EU Article 29 Working Party Guidance Under the Present System

The EU's Article 29 Working Party (the "WP29"), an independent advisory panel, gives guidance on privacy directives to member states, which then can be used by member state data protection agencies or legislators.[16] The guidance may also be referred to by practitioners to anticipate member state application of the Directive to new issues, such as those raised by data processing for new uses or using new technologies.

Three of the various areas on which the WP29 gave guidance the past year are addressed below:

1. Consent

The meaning of consent impacts both the Directive and the ePrivacy Directive.[17] This survey is limited to the former.

12. *Id.* ¶ 43 (citing Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 2008 E.C.R. I-271, [2008] 2 C.M.L.R. 17). For a discussion of the *Promusicae* case, see Siegel et al., *supra* note 3, at 306.

13. *ASNEF*, [2012] 1 C.M.L.R. 48, ¶ 48.

14. *Id.* ¶¶ 43–49.

15. S.T.S., Feb. 8, 2012 (No. 429) (Spain), *available at* http://www.poderjudicial.es/search/sentencias/proteccion%20de%20datos%20de%20caracter%20personal/1/PUB. For a discussion of this annulment in English, see Belén Gámez, *Spanish Supreme Court Annuls Limitation on Processing of Personal Data*, Hogan Lovells Chron. of Data Protection (Feb. 29, 2012), http://www.hldataprotection.com/2012/02/articles/international-eu-privacy/spanish-supreme-court-annuls-limitation-on-processing-of-personal-data/.

16. *See Article 29 Working Party*, Eur. Commission, http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (last updated Feb. 3, 2012).

17. Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC) (Directive on Privacy and Electronic Communications, commonly known as the "ePrivacy Directive").

Under the Directive, consent is used as a basis for the lawfulness of data processing, and "explicit" consent is used to legitimize processing of "sensitive" data.[18] This consent must, as a general rule, be expressed prior to the beginning of the data processing and be unambiguous,[19] and the data processing must be transparent.[20]

Consent includes "any indication of a wish, by which the data subject *signifies* his agreement,"[21] whether by a handwritten signature, an oral statement, or behavior. In general, this behavior must be an action; that is, it cannot be inaction or "passive behaviour."[22]

The consent of the data subject must be "freely given"—not obtained through deception, coercion, intimidation, or risk of "significant negative consequences if he/she does not consent."[23] Certain categories of the processing of personal data may not be legitimized merely by consent, such as in the case where the data subject is in an employment relationship with the data controller, and thereby cannot freely withhold consent (absent "sufficient guarantees" that the consent is given freely).[24]

The purposes of data processing must be specified in order to obtain consent to such processing.[25] The consent can be accorded only for a limited set of data processing activities, although that may include different operations if "within the reasonable expectations of the data subject."[26]

Finally, the consent must be "informed."[27] The data subject must have information—such as his or her rights, the reasons for and nature of the data processing, and the identity of potential transferees of the data.[28] The information must be intelligible and accessible (not just "available" somewhere).[29]

Firms should ensure that consent for processing personal data is legitimate and adequate for the kind of data being processed. Sufficient, clear, and accessible information about the data processing must be given to data subjects. Businesses should review their privacy policies, contracts, general terms of use, and other documentation in this light.

18. *See* Article 29 Data Prot. Working Party, Opinion 15/2011 on the Definition of Consent 6 (July 13, 2011) (WP 187), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf. The consent may be expressed through a handwritten or electronic signature or writing, or by oral agreement, but may not generally be inferred. *See id.* at 25. Opt-out procedures will not be considered explicit. *See id.*

19. In order to be unambiguous, there must be no doubt as to the intent of the data subject to give his or her consent. *Id.* at 21. This is achieved through the use of robust procedures and the retention of evidence of intent. *See id.*

20. *Id.* at 9–10.

21. *Id.* at 11.

22. *Id.* at 12.

23. *Id.*

24. *Id.* at 12–14.

25. *Id.* at 17–19.

26. *Id.* at 17.

27. *Id.* at 19.

28. *Id.*

29. *Id.* at 19–20.

2. Facial Recognition in Online and Mobile Services

The WP29's opinion on facial recognition in online and mobile services[30] refers to the relevant processing as one of using personal data (whether it be a digital image of a face or a "reference template" created from such an image and used for future identification and comparison), subject to the Directive.[31] As a result, the processing may occur only if "legitimate" within the context of Article 7 of the Directive.[32] Furthermore, the WP29 considered the particular risks associated with biometric data, and accordingly, generally requires "informed consent of the individual prior to commencing the processing of digital images for facial recognition,"[33] except in certain cases where there is a need for the data controller to perform some preliminary facial recognition processing—for example, in order to determine whether the data subject has given consent or not.[34]

Information regarding the facial recognition processing must be clear and easily available; consent must be specific prior to enrollment, unless it is clear that the service's primary purpose involves facial recognition.[35] The recommendations of the WP29 highlight the importance of the data controller ensuring the security of data during transit, including through encrypted communication channels or even encrypting individual images and templates.[36]

Special care must be taken when providing facial recognition services, and data security must be ensured. Specific prior informed consent to the processing generally should be required before providing such services.

3. Biometric Technologies

On April 27, 2012, the WP29 adopted its opinion on developments in biometric technologies.[37] The opinion emphasizes the specific danger of biometric technologies to data protection and privacy because of the linkage of the technologies to "certain characteristics of an individual."[38] The WP29 states that "biometric data are in most cases personal data,"[39] therefore subject to the Directive framework, and that they may be processed only if legitimate under the Directive.[40] In accordance with the Directive, biometric data subjects must know of

30. Article 29 Data Prot. Working Party, Opinion 2/2012 on Facial Recognition in Online and Mobile Services (Mar. 22, 2012) (WP 192), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf.

31. *Id.* at 4.

32. *Id.* at 5.

33. *Id.*

34. *Id.*

35. *Id.* at 7.

36. *Id.* at 8.

37. Article 29 Data Prot. Working Party, Opinion 3/2012 on Developments in Biometric Technologies (Apr. 27, 2012) (WP 193), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

38. *Id.* at 3.

39. *Id.* at 7.

40. *Id.* at 10–13 (referencing the grounds for legitimacy).

the collection or use of their data, have access to it, and it must be properly secured.[41] The purpose of the biometric data processing must be clearly defined and limited, based on principles of proportionality (non-excessiveness), necessity, and "data minimization" (only the required information being processed).[42]

The WP29 underscores the importance of biometric data security, and recommends "a high level of technical protection for . . . processing [as well as the use of] privacy by design."[43] In addition to calling for a risk analysis or dedicated "Privacy Impact Assessment (PIA)" for biometrics systems conceived as part of the design stage by the party defining the purpose of the system (e.g., the manufacturer, integrator, or final client), the WP29 encourages the development of certification schemes.[44] Special risks relating to biometrics data that are to be analyzed in the PIA are identity theft, improper use of the data ("purpose diversion"), and data breaches.[45] The WP29 sets out different technical measures that may be adopted to protect against these risks (e.g., use of encryption technologies, storage of data on personal devices such as smart cards instead of centralized storage, and establishment of automated data erasure mechanisms to delete data no longer needed).[46]

Thus, because of the special nature of biometric technologies, which are closely linked to individuals' personal characteristics, the WP29 has emphasized the importance of data security, and has suggested various ways by which security risks may be addressed.

III. Legislative Proposals

On January 25, 2012, Viviane Reding, EU Justice Commissioner and Vice President of the European Commission, introduced two proposed laws to reform the Directive framework[47]: (i) a proposed directive relating to data processing by authorities in connection with criminal matters,[48] and (ii) a proposed regulation relating to general data protection (the General Data Protection Regulation, hereinafter "GDPR").[49] This survey focuses on the latter.

41. *Id.* at 14.

42. *Id.* at 7–10.

43. *Id.* at 28. "Privacy by design" is defined as "the concept of embedding privacy proactively into technology itself." *Id.*

44. *Id.* at 29.

45. *Id.* at 30–31.

46. *Id.* at 31–33.

47. Press Release, Eur. Comm'n, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses (Jan. 25, 2012), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=1&language=EN&guiLanguage=en.

48. *Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offenses or the Execution of Criminal Penalties, and the Free Movement of Such Data*, COM (2012) 10 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf.

49. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (General

The GDPR will interest non-EU practitioners and firms, as well as Europeans, as in its current form it would apply even to controllers not established in the EU, provided that they engage in data processing of EU residents' personal data, where such processing is related to the offer of goods or services in the EU or to behavior monitoring.[50] In such cases, a controller located outside of the EU may have to appoint a representative in the EU, who may be addressed on the controller's behalf by a supervisory authority, if the controller meets the criteria set out in the GDPR.[51] This is in addition to the obligation for certain controllers and processors of personal data, when required, to designate a data protection officer, who is either an employee or someone engaged by the controller or processor through a service contract.[52]

The GDPR, which may possibly come to a vote of the European Parliament in plenary session in early 2014, was proposed for various reasons, with some of the main ones summarized below.

A. Greater Harmonization

The fragmentation of EU personal data protection has been decried, often due to legal uncertainty, lack of harmonization, and complexity.[53] These perceived flaws are considered impediments to business in a globalized world.[54] A single legal instrument in the form of a regulation is thought to be the way to establish the necessary data protection framework and to harmonize the law while simultaneously allowing direct applicability throughout the EU.[55]

B. Dealings with One National Data Protection Authority

Article 51(2) of the proposed GDPR provides that, where a personal data controller or processor is established in more than one member state, "the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States."[56] The GDPR provides for cooperation and mutual assistance between supervisory authorities,[57] and would establish a "consistency mechanism," involving a European Data Protection Board.[58]

Thus, a controller or a processor would deal with their home supervisory authority, saving time and money, but consistency among the various authorities

Data Protection Regulation), COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

50. *Id.* art. 3(2), at 41.
51. *Id.* art. 25, at 56–57.
52. *Id.* art. 35, at 65–66.
53. *Id.* at 4.
54. *Id.*
55. *Id.* at 5–6. An EU regulation, unlike a directive, does not need to be implemented by each member state to become effective. *See id.* at 6.
56. *Id.* art. 51(2), at 77.
57. *Id.* arts. 55–56, at 80–82.
58. *Id.* arts. 57–63, at 82–86.

of the different member states would be ensured through a mechanism foreseen under the GDPR.

C. Increased Data Breach Requirements; Accountability and Responsibility

Several requirements are placed upon the data controller or processor, including the implementation of security measures and a notification requirement to the supervisory authority of personal data breaches "without undue delay and, where feasible, not later than 24 hours after having become aware of [any such breach]."[59] If notification occurs after twenty-four hours, a "reasoned justification" must be provided.[60] A processor must "alert and inform the controller immediately after the establishment" of a breach,[61] and a controller must communicate a breach to a data subject "without undue delay" if the breach is "likely to adversely affect the protection of the personal data or privacy of the data subject,"[62] but shall not be so required if it can prove to the supervisory authority's satisfaction that it had implemented protections rendering the data "unintelligible to any person who is not authorised to access it."[63]

Increased data breach requirements are just part of the increased accountability and responsibility requirements for personal data controllers under the GDPR; they include carrying out a data protection impact assessment, or obtaining prior authorization in certain circumstances, for example.[64]

D. Data Portability

Article 18 establishes a right to data portability, through allowing the data subject to obtain his or her personal data and transmit them into another data processing system in a commonly used electronic format, without hindrance.[65]

E. Right to Be Forgotten

The data subject has a right to require the controller to erase his or her personal data under certain grounds set out in Article 17(1), including where the data are no longer needed for the original purpose, where the data subject exercises his or her right to object, or where he or she "withdraws consent on which the processing is based."[66]

59. *Id.* art. 31(1), at 60.
60. *Id.*
61. *Id.* art. 31(2), at 60.
62. *Id.* art. 32(1), at 61.
63. *Id.* art. 32(3), at 61–62.
64. *Id.* arts. 33–34, at 62–64.
65. *Id.* art. 18(1)–(3), at 53.
66. *Id.* art. 17(1), at 51.

F. Increased Fines

Article 79 of the proposed GDPR would establish a sliding scale of fines based on whether one's first violation was "non-intentional non-compliance," and whether or not the violator is an enterprise (and then, whether or not a small enterprise).[67] The fine may be based upon the duration, nature, and gravity of the offense, and could reach a maximum of 2 percent of annual worldwide turnover for certain intentional or negligent breaches by an enterprise.[68] Thus, the proposed GDPR could result in sharply increased fines.

IV. Conclusion

Throughout the year developments in EU privacy law have tended to limit divergence from European law, to encourage convergence in the application of laws through guidance, or to update law by dealing with new technologies and uses of data processing. The proposed GDPR can be seen as a culmination of these trends, by allowing for potential unification of law, by incorporating many of the principles (e.g., transparency and data minimization) and advances developed through WP29 guidance, and by bringing the Directive (in a new form) into the twenty-first century. Firms should make an effort now to understand the proposed GDPR and to initiate relatively long lead-time measures (such as privacy by design, or certain security actions) in anticipation of the GDPR's possible application.

67. *Id.* art. 79, at 92–94.
68. *Id.*

The EU E-Privacy Directive and Consent to Cookies

*By Robert Bond**

Background

Under the previous legal regime, the use of cookies[1] was governed by Article 5(3) of the European Union E-Privacy Directive ("E-Privacy Directive") concerning the processing of personal data and the protection of privacy in the electronic communications sector.[2] The storing of cookies was allowed only if the user was "provided with clear and comprehensive information . . . about the purposes of the processing and [was] offered the right to refuse such processing by the data controller."[3] As such, the former regime on cookies was an informed opt-out approach.

In 2009, Article 5(3) of the E-Privacy Directive was amended ("2009 Directive"), changing the notice and consent requirements from informed opt-out to an almost (but not quite) informed opt-in.[4] Subject to a very limited exception (the "strictly necessary" cookies), the use of cookies will be allowed only if the user has given consent after being provided with clear and comprehensive information about why his or her data is being tracked.[5]

---

* Robert Bond is a Partner, Notary Public, and Certified Compliance and Ethics Professional with the international law firm Speechly Bircham LLP in its London office, where he heads the Data Protection and Informational Law team. He also led the legal drafting of the International Chamber of Commerce United Kingdom Cookie Guide with other experts including his son Mike Bond, International Chamber of Commerce United Kingdom Digital Economy Policy Advisor.

1. Cookies are uniquely assigned to users and can only be read by the host that provided that cookie to that user. *Description of Cookies*, Microsoft.com (May 10, 2012), http://support.microsoft.com/kb/260971. Cookies cannot be used to run code/programs on a user's computer, nor can they be used to deliver viruses. *Id.* First-party cookies are set by the website owner and are commonly used to store information, e.g., user preferences, such as a login name. *Understanding Cookies*, Microsoft.com, http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sec_cook.mspx?mfr=true (last visited July 21, 2012). They can be either persistent or session cookies. *Cookies: Frequently Asked Questions*, Microsoft.com, http://windows.microsoft.com/en-GB/windows7/Cookies-frequently-asked-questions (last visited July 21, 2012). Then there are third-party cookies that come from other websites or web services that may be connected to the first-party cookie website. *Id.* They often track webpage usage for advertising or other marketing purposes. *Id.* They deliver advertising content into a webpage from somewhere outside that website (such as "sponsored links" columns or banner advertising networks), and they also can be either persistent or session cookies. *Understanding Cookies*, Microsoft.com, http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sec_cook.mspx?mfr=true (last visited July 21, 2012).

2. Council Directive 2002/58 art. 5(3), 2002 O.J. (L201) 37, 44 (EC).

3. *Id.*

4. Council Directive 2009/136 art. 2(5), 2009 O.J. (L337) 11, 30 (EC).

5. *Id.*

In addition, by Recital 66 of the 2009 Directive, consent to cookies "may be expressed by using the appropriate settings of a browser or other application."[6] The 2009 Directive now states the following:

> Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, *inter alia*, about the purposes of the processing.[7]

It should be remembered that there is also the following useful wording:

> This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.[8]

Member states should have implemented the revisions to the E-Privacy Directive by May 25, 2011.[9]

However, the situation is confused for these reasons:

- Each of Austria, Italy, France, Belgium, Finland, Spain, Portugal, Sweden, Latvia, Lithuania, Netherlands, Ireland, Luxembourg, Hungary, Malta, United Kingdom, Slovenia, and Estonia passed a new law to comply, or decided that its existing laws already complied, with the 2009 Directive.[10]
- The United Kingdom gave businesses twelve months to become compliant before enforcement began on May 26, 2012.[11]
- Other member states are still drafting legislation or have made no decision regarding the compliance of their existing laws with the requirements of the 2009 Directive.
- There is no clear harmonized guidance as to how consent is to be given or obtained. Browser solutions are still a work in progress, although several member state laws anticipate them as a solution to "consent."[12]

6. *Id.* at 20.
7. *Id.* at 30.
8. *Id.*
9. *Id.* at 32.
10. *National Execution Measures*, ACCESS TO EUROPEAN UNION LAW, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:72009L0136:EN:NOT (last visited July 21, 2012).
11. Press Release, Info. Commissioner's Office, ICO Gives Website Owners One Year to Comply with Cookies Law (May 25, 2011), *available at* http://www.ico.gov.uk/news/latest_news//media/documents/pressreleases/2011/enforcement_cookies_rules_news_release_20110525.ashx.
12. *Cookies: New EU Cookie Law (e-Privacy Directive)*, INFO. COMMISSIONER'S OFFICE, http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.asx (last visited July 21, 2012).

These issues aside, website operators should take note that the new cookies law applies to any website that uses cookies irrespective of whether it is controlled by a business within or outside the European Union.[13] Thus, there is direct applicability of this legislation to U.S. corporations that operate websites that are visited by users in the European Union. Because the legislation is not prescriptive about user equipment, it applies to web browsing on a desktop, a laptop, a tablet, or a smartphone.

How to Get Consent

The Article 29 Data Protection Working Party[14] provides a useful analysis on the meaning of consent in its 2011 opinion.[15] The opinion states the following:

- "Consent is one of several legal grounds to process personal data. It has an important role, but this does not exclude the possibility, depending on the context, of other legal grounds perhaps being more appropriate from both the controller's and from the data subject's perspective."[16]
- "[O]btaining consent does not negate the controller's obligations under Article 6 [of the E-Privacy Directive] with regard to fairness, necessity and proportionality, as well as data quality."[17]
- "The notion of control is also linked to the fact that the data subject should be able to withdraw his consent."[18]
- "Transparency is a condition of being in control and for rendering the consent valid."[19]
- "Although the timing for seeking consent is not spel[led] out in the [E-Privacy] Directive, it is clearly implied from the language of the various provisions which indicate that, as a general rule, consent has to be given before the processing starts."[20]

13. Info. Commissioner's Office, Guidance on the Rules on Use of Cookies and Similar Technologies 14 (2012) [hereinafter ICO's Guidance], *available at* http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx (follow "cookies guidance (pdf)" hyperlink).

14. The Article 29 Data Protection Working Party consists of representatives of the Data Protection Authorities in the European Union. *See Article 29 Working Party*, Eur. Commission, http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (last updated Feb. 3, 2012).

15. Article 29 Data Prot. Working Party, *Opinion 15/2011 on the Definition of Consent* 2 (July 13, 2011) (WP 187), *available at* http://www.ico.gov.uk/news/latest_news/~/media/documents/pressreleases/2011/enforcement_cookies_rules_news_release_20110525.ashx.

16. *Id.*

17. *Id.* at 7.

18. *Id.* at 9.

19. *Id.*

20. *Id.*

French and U.K. Guidance on Cookies

In response to the 2009 Directive, the French government implemented Ordinance No. 2011-1012 on August 24, 2011.[21] The French Supervisory Authority (CNIL) subsequently published guidance in relation to the 2009 Directive and France's ordinance regarding cookies.[22] According to CNIL's guidance, when referring to consent, the French translation of the 2009 Directive and the French legislative order specifically use words that mean "permission" or "agreement" in English.[23] To that end, the use of the words "permission" or "agreement" still refers to "consent as defined in article 2(h) of Directive 95/46/EC, that is to say . . . 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.' "[24]

The United Kingdom's response to the 2009 Directive came in the form of the cookies guidance from the Information Commissioner's Officer ("Guidance")[25] and the Cookie Guide from the International Chamber of Commerce United Kingdom ("Guide").[26] The Guidance stated, "Consent must involve some form of communication where the individual knowingly indicates [his or her] acceptance. This may involve clicking an icon, sending an email or subscribing to a service. The crucial consideration is that the individual must fully understand that by the action in question [he or she] will be giving consent."[27] The Guidance further stated the following:

> The level of consent required for any activity has to take into account the degree of understanding and awareness the person being asked to agree has about what they are consenting to. A reliance on implied consent in any context must be based on a definite shared understanding of what is going to happen—in this situation a user has a full understanding of the fact cookies will be set, is clear about what cookies do and signifies [his or her] agreement. At present evidence demonstrates that general awareness of the functions and uses of cookies is simply not high enough for websites to look to rely entirely in the first instance on implied consent.[28]

21. Loi 2011-1012 du 24 août 2011 relative aux communications électroniques [Law 2011-1012 of August 24, 2011 on Electronic Communications], Journal Officiel de la République Française [J.O.] [Official Gazette of France], Aug. 26, 2011, p. 14473, *available at* http://www.steptoe.com/assets/attachments/4307.pdf.

22. *What the Telecoms Package Changes for Cookies*, Commission Nationale de L'Informatique et des Libertés (Dec. 20, 2011), http://www.cnil.fr/english/news-and-events/news/article/what-the-telecoms-package-changes-for-cookies/.

23. *Id.*; Gabriel Voisin, *CNIL Releases Cookie Guidance*, IAPP (Nov. 4, 2011), https://www.privacyassociation.org/publications/cnil_releases_cookie_guidance.

24. *What the Telecoms Package Changes for Cookies*, Commission Nationale de L'Informatique et des Libertés (Dec. 20, 2011), http://www.cnil.fr/english/news-and-events/news/article/what-the-telecoms-package-changes-for-cookies/.

25. ICO's Guidance, *supra* note 13, at 5–6.

26. Int'l Chamber of Commerce U.K., ICC UK Cookie Guide 2 (2012) [hereinafter ICC's Guide], *available at* http://www.international-chamber.co.uk/components/com_wordpress/wp/wp-content/uploads/2012/04/icc_uk_cookie_guide.pdf.

27. ICO's Guidance, *supra* note 13, at 5–6.

28. Info. Commissioner's Office, Guidance on the Rules on Use of Cookies and Similar Technologies (2d ed. 2011) (on file with *The Business Lawyer*).

The latest guidance on the ICO website states that "[i]f you are relying on implied consent you need to be satisfied that your users understand that their actions will result in cookies being set. Without this understanding you do not have their informed consent."[29]

The goal of the Guide is to help both website operators and website users understand the so-called cookies law by dividing cookies into four categories based on their functions.[30] The Guide is intended to help website operators categorize the cookies they use and assist the website operators in preparing suitable methods of obtaining informed consent, as well as aiding communication with website visitors by offering them standard notice language explaining in simple terms what cookies are and how they are used.[31] The International Chamber of Commerce United Kingdom hopes that the Guide will be adopted by businesses across the European Union so that repeated use of standard language will provide certainty and comfort for consumers.[32] The Guide was developed through consensus and compromise among many leading businesses that provided technical, marketing, or legal input to ensure a rounded solution.[33]

At the launch of the Guide at an event hosted by, the Department for Culture, Media and Sport and the Information Commissioners Office in London, Department Minister Ed Vaizey confirmed that "'we will lead the way forward' in influencing, at [the] ministerial level across Europe, the need for an harmonised approach to compliance."[34] Christopher Graham, U.K. Information Commissioner, also commended the International Chamber of Commerce, adding, "we are seeing lots of good work—but until it all ends up on websites there is a risk that bluster, scare tactics and burying of heads will win the day . . . and from May [2012] we will shift our response to those businesses who will not comply or attempt to comply."[35]

So What Does the Guide Achieve?

The Guide is based on the fact that different cookie technologies have been categorized into four groups around their functions and their use.[36] While these categorizations may be changed as the International Chamber of Commerce United Kingdom continues its consultation with stakeholders, the four categories that have been identified and approved by the Information Commissioner's Office are as follows:

29. *Cookies*, Info. Commissioner's Office, http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx (last visited Sept. 6, 2012).
30. ICC's Guide, *supra* note 26, at 2.
31. *Id.*
32. *Id.*
33. *See id.* at 14.
34. Robert Bond, *ICC UK Cookie Guide: Taking the Biscuit*, Soc'y for Computers & L. (Apr. 4, 2012), http://www.scl.org/site.aspx?i=ed26002.
35. *Id.*
36. ICC's Guide, *supra* note 26, at 3.

1. Strictly necessary cookies;
2. Performance cookies;
3. Functionality cookies; and
4. Targeting or advertising cookies.[37]

Part One of the Guide explains its general purposes for website operators, and Part Two then sets out in more detail the explanations with case studies of the four categories of cookies.[38] Part Three contains technical notes and definitions in relation to the four categories of cookies,[39] and Part Four gives some examples of how consent might be obtained.[40] The Guide is not intended to provide legal advice, and website operators are responsible, of course, for their own compliance strategies depending on the cookies they use and the nature of their websites and its users.[41]

Categories of Cookies[42]

As it is important that consent be meaningful when required for the use of cookies, it is essential to have plain language explanations of the technical de-

37. *Id.*
38. *Id.* at 3–9.
39. *Id.* at 10–12.
40. *Id.* at 12–13.
41. *Id.* at 2.
42. Temporary cookies, also called transient cookies or session cookies, are used to store only temporary information and are deleted when an internet browsing session ends (i.e., when you close your browser such as Firefox or Safari). *Understanding Cookies*, Microsoft.com, http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sec_cook.mspx?mfr=true (last visited July 21, 2012). These cookies include a unique session ID that does not personally identify users. Vangie Beal, *What Are Cookies and What Do Cookies Do?*, Webopedia, http://www.webopedia.com/DidYouKnow/Internet/2007/all_about_cookies.asp (last updated Aug. 31, 2010). Then there are persistent cookies or "stored"/"saved" cookies that enhance or streamline the user experience by storing preferences or user data: websites use them to store information such as the sign-in name so people do not have to sign-in again when returning to a website. *Cookies: Frequently Asked Questions*, Microsoft.com, http://windows.microsoft.com/en-GB/windows7/Cookies-frequently-asked-questions (last visited July 21, 2012). Another example of a persistent cookie is choosing a language on a first visit and, once selected, a persistent cookie remembers that option. *What Are Persistent Cookies Used For?*, All About Cookies, http://www.allaboutcookies.org/cookies/persistent-cookies-used-for.html (last visited July 21, 2012). Persistent cookies stay on the hard drive after the current browsing session until they are erased by the user or expire at the time set by the web server that issued them. *About Cookies*, All About Cookies, http://www.allaboutcookies.org/cookies/cookies-the-same.html (last visited July 21, 2012). A common use is to help websites analyze users' online behavior, providing customer insight. *See Privacy and Security*, Gen. Servs. Admin., http://publications.usa.gov/USAPubs.php?NavCode=N (last visited July 21, 2012).

Another example of cookies are flash cookies or "local shared objects" that are software files created using the "flash" authoring tool and devised to get around the challenge of cookie deletion. *See* Ashkan Soltani et al., *Flash Cookies and Privacy* 1 (Aug. 10, 2009), *available at* http://ssrn.com/abstract=1446862. By design they are more invasive and do not show up in a user's browser. *See id.* They work in a different way than the temporary or persistent HTTP cookies but give a benefit to websites that is similar to the benefits of persistent HTTP cookies. *See generally id.* They have the instructions and the ability to recreate HTTP cookies after deletion. *See id.* at 2. Websites that want browsers to continue to be identifiable by a server reinstall deleted regular HTTP cookies

scription of cookies but in such a way that compliance can be legally achieved.[43] While four categories have been chosen, it is quite possible that a cookie may function in more than one category, necessitating consent for each applicable category.[44] Therefore, the way in which the categories are used and the consent language applied will vary depending entirely upon each website.

Strictly Necessary Cookies

The Guide states that a notice for users about strictly necessary cookies might be worded as follows: "These cookies are essential in order to enable you to move around the website and use its features, such as accessing secure areas of the website. Without these[,] cookies services you have asked for, like shopping baskets or e-billing, cannot be provided."[45] In its Guide, the International Chamber of Commerce United Kingdomin dicates the range of different technologies that may be categorized as cookies and also provides simple "Tool Tips" for consumer understanding.[46] For example, the strictly necessary cookie Tool Tip states: "These cookies enable services you have specifically asked for."[47]

Performance Cookies

For performance cookies, the notice for users might read:

> These cookies collect information about how visitors use a website, for instance which pages visitors go to most often, and if they get error messages from web pages. These cookies don't collect information that identifies a visitor. All information these cookies collect is aggregated and therefore anonymous. It is only used to improve how a website works.[48]

The Tool Tip here is that "[t]hese cookies collect anonymous information on the pages visited."[49]

Functionality Cookies

The notice for users regarding functionality cookies is more detailed given the more complex nature of functionality cookies. The suggested notice for functionality cookies essentially gives examples of use, including "choices you make (such as your user name, language or the region you are in)[,] and provide[s] enhanced, more personal features."[50]

---

even when a person has deliberately deleted the cookie, which is called re-spawning. *Id.* at 2 & n.1. They can contain up to 100kb of data, versus the 4kb that an HTTP cookie can store. *Id.* at 1.

43. ICC's Guide, *supra* note 26, at 6.
44. *Id.*
45. *Id.* at 7.
46. *Id.*
47. *Id.*
48. *Id.*
49. *Id.* at 8.
50. *Id.*

The Tool Tip here is that "[t]hese cookies remember choices you make to improve your experience."[51]

Targeting Cookies or Advertising Cookies

Finally, what falls into the online behavioral advertising sector in some respects or customer profiling is what the International Chamber of Commerce United Kingdom calls targeting cookies or advertising cookies. The suggested notice for users reads:

> These cookies are used to deliver adverts more relevant to you and your interests. They are also used to limit the number of times you see an advertisement as well as help measure the effectiveness of the advertising campaign. They are usually placed by advertising networks with the website operator's permission. They remember that you have visited a website and this information is shared with other organisations such as advertisers. Quite often targeting or advertising cookies will be linked to site functionality provided by the other organisation.[52]

The Tool Tip here is that "[t]hese cookies collect information about your browsing habits in order to make advertising relevant to you and your interests."[53] It is valuable for businesses to note that each of the descriptions of cookies is couched in positive language to allay users' fears, provide plain language information, and not cause rejection of any of the cookie categories.

Consent

In Part Four of the Guide, sample consent language is provided to dovetail with the cookie categories.[54] The "strictly necessary" cookies do not require consent,[55] although the Information Commissioner's Office, and indeed the guidance from the U.K. Information Commissioner's Office, recommend that cookie information be provided.[56] In the other three categories, the mechanisms of obtaining consent are interpreted on a sliding scale of impact and effect.[57] In other words, the more pervasive the use of the cookie in terms of collecting data, the greater the need to demonstrate explicit consent.

While a user need not consent to a "strictly necessary" cookie, consent might be implied by the user's continued use of the website after having been offered a chance to understand that category of cookie. This implied-consent argument is bolstered by the fact that strictly necessary cookies gather little personal data and, in any event, the aggregation of the information is used only to enhance future performance of the website. At the other end of the scale, for advertising

51. *Id.*
52. *Id.*
53. *Id.*
54. *Id.* at 12–13.
55. *Id.* at 7, 12.
56. *See* ICO's Guidance, *supra* note 13, at 12–13.
57. ICC's Guide, *supra* note 26, at 12–13.

cookies, the mechanism of obtaining consent needs to be the most transparent and effective.

Conclusion

The Guide is timely, practical, and current, in the absence of any more definitive guidance from either government or regulators. It remains to be seen how the law will be enforced. Failure to comply can carry significant fines in some European Union member states (up to £500,000 in the United Kingdom), as well as enforcement proceedings and "naming and shaming."[58] More important, a business that is investigated for non-compliance with the E-Privacy Directive cookies law may find itself subjected to far greater scrutiny.

58. ICO's Guidance, *supra* note 13, at 26–27.

Survey of Recent FTC Privacy Enforcement Actions and Developments

*By Fatima Nadine Khan**

Introduction

The rapidly changing pace of technology has presented challenges to both businesses and consumers in reconciling privacy and business interests. This survey continues from last year's survey[1] delineating major developments by the Federal Trade Commission ("FTC") to protect consumer privacy. It sets out the FTC's recent enforcement actions, privacy reports by the agency, and further initiatives by the agency to address privacy.

FTC Enforcement Actions

Recently, the FTC has steadily increased the number of enforcement actions for privacy violations including bringing its first case against a developer of a mobile application for a privacy violation in September 2011.[2]

Myspace

In the FTC's case against Myspace, the FTC showed concern for notice and choice. Myspace is a social networking service that allows users to create a customized online profile containing personal information.[3] Each Myspace profile is assigned a unique, persistent identifier, or "Friend ID."[4] Contrary to representations in its privacy policy, Myspace shared the Friend IDs with third-party advertisers not affiliated with Myspace, resulting in violations of user privacy.[5] The practice allowed a third party to access a user's personal information or to identify individual users.[6] Additionally, web-browsing activity shared with

* Fatima Khan primarily practices in the areas of technology transactions and privacy.

1. Fatima Khan, *Survey of Recent FTC Privacy Developments and Enforcement*, 67 Bus. Law. 297 (2011).

2. Press Release, Fed. Trade Comm'n, Mobile Apps Developer Settles FTC Charges It Violated Children's Privacy Rule (Aug. 15, 2011), *available at* http://www.ftc.gov/opa/2011/08/w3mobileapps.shtm.

3. Complaint ¶ 3, *In re* Myspace LLC, No. 102-3058, 2012 WL 1745313 (FTC May 8, 2012).

4. *Id.* ¶ 4.

5. *Id.* ¶¶ 11–13.

6. *Id.* ¶ 13.

advertisers was not anonymized as represented in the policy.[7] As a result, the FTC charged Myspace with three violations of section 5 of the FTC Act for false, misleading, or deceptive practices and a violation of the US-EU Safe Harbor privacy principles of "notice" and "choice."[8]

RockYou

In the RockYou case, the FTC showed concern for privacy by design.[9] RockYou operates a website that allows users to create content that can be published through a widget and shared across different platforms.[10] Contrary to the representations in its privacy policy to take reasonable security safeguards, RockYou failed to take reasonable data security measures in collecting consumers' personal e-mail address passwords, storing passwords in clear text, not segmenting its servers, and not protecting its website against foreseeable data security attacks.[11] These practices led to the unauthorized access to approximately 32 million e-mail addresses and RockYou passwords and the access to account information that users chose to keep private.[12] In the course of the data collection, RockYou also collected and exposed information from approximately 179,000 children.[13] In addition to untrue security claims, the RockYou privacy policy falsely claimed to delete information of children knowingly collected.[14]

As a result of these practices, the FTC charged RockYou with violating the Children's Online Privacy Protection Act ("COPPA") Rule as well as section 5 of the FTC Act for data security (not privacy) and the collection and retention of personal information from children.[15]

Upromise

In the Upromise case, the FTC showed concern for privacy by design and transparency. Upromise is a membership-based program that allows consumers

7. *Id.* ¶ 14.
8. *Id.* ¶¶ 15–28.
9. "Privacy by design" consists of encouraging companies to "promote consumer privacy throughout their organizations and at every stage of the development of their products and services." There are two elements to the implementation of "privacy by design": (a) the incorporation of substantive privacy practices, like data security, sound data retention practices, and data accuracy; and (b) comprehensive data management procedures utilized during all stages of products and services. Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Preliminary FTC Staff Report) 41 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
10. Complaint for Civil Penalties, Permanent Injunction, and Other Relief ¶ 12, United States v. RockYou, Inc., CV 12 1487 (N.D. Cal. Mar. 26, 2012), *available at* http://www.ftc.gov/os/caselist/1023120/120327rockyoucmpt.pdf.
11. *Id.* ¶ 16.
12. *Id.* ¶ 17.
13. *Id.* ¶ 20.
14. *Id.* ¶ 23.
15. *Id.* ¶¶ 23–36.

to receive cash rebates for college savings for specific purchases.[16] Through the program, Upromise offered a toolbar that incorporated a "personalized offers" feature.[17] This feature targeted advertising based upon consumer browsing information.[18] Contrary to the statements in the privacy policy regarding privacy filters, "infrequent" collection of personal information, and data security, the tool collected vast amounts of identifiable personal data and transmitted the data in clear text.[19] The FTC charged Upromise with a violation of section 5 of the FTC Act based on the failure to disclose the extent of information collected, unreasonable data security practices, and the failure to take appropriate measures to protect consumers' data.[20]

Facebook

In its action against Facebook, the FTC showed concern for choice, transparency, and privacy by design. Facebook operates a social networking service that allows users to create online profiles containing information about the user, and also operates the Facebook Platform, which consists of tools and programming interfaces that allow third parties to develop and run applications for Facebook users.[21] Facebook gains revenue through selling advertising and Facebook Credits, a virtual currency.[22]

First, although Facebook has given its users the ability to restrict privacy settings to specific groups, its privacy setting options failed to disclose that a user's privacy settings would be ineffective as to specific third parties, such as particular applications on the Facebook Platform.[23] Second, in December 2009, Facebook changed its privacy policy without warning, resulting in changes that affected the privacy of users. Such changes included (1) overriding the existing privacy settings of users; (2) making certain private information "publicly available" to applications, changing access to a user's "friend" list, and altering picture and profile visibility in search engines; (3) representing to provide greater privacy control and failing to disclose changes that overrode settings; and (4) materially changing promises to keep information private.[24] Third, Facebook claimed that applications would only have access to information needed to operate; however, applications could access information unrelated to their purpose or operation.[25] Fourth, Facebook shared personal information with

16. Complaint ¶ 3, *In re* Upromise, Inc., No. 102-3116, 2012 WL 1225058 (FTC Mar. 27, 2012).
17. *Id.* ¶¶ 4–5.
18. *Id.* ¶ 5.
19. *Id.* ¶¶ 6–14.
20. *Id.* ¶¶ 15–21.
21. Complaint ¶¶ 1–2, *In re* Facebook, Inc., No. 092-3184, 2011 WL 7096348 (FTC Nov. 29, 2011).
22. *Id.* ¶ 2.
23. *Id.* ¶¶ 10–18.
24. *Id.* ¶¶ 19–29.
25. *Id.* ¶¶ 30–31.

third-party advertisers in spite of representations to the contrary.[26] Fifth, Facebook created a "Verified Apps" program for which it claimed to certify and review the security of an application with such a status; however, Facebook did not take any steps to verify the security of the participating applications.[27] Sixth, Facebook claimed that once users deactivated or deleted their accounts, their photos and videos would not be accessible to other users; however, this information was available via Content URLs.[28] For the above reasons, the FTC alleged that Facebook violated section 5 of the FTC Act and failed to comply with the US-EU Safe Harbor principles, especially notice and choice principles.[29]

Skid-e-kids

In this action, the FTC showed concern for privacy by design and notice. Skid-e-kids is a social networking site for children that lets users create profiles, befriend others, play games, and write messages, among other activities.[30] Contrary to the website's privacy policy, the website collects children's information at the point of registration without making any attempt to notify parents or ask for a parent's e-mail address.[31] The website's privacy notices also did not fully or accurately disclose data collection and use of children's information.[32] In the course of business, Skid-e-kids collected information from approximately 5,600 children.[33] The FTC charged the website owner-operator with a violation of section 5 of the FTC Act for its false privacy policy claims and a violation of COPPA.[34]

W3 Innovations

In this action, the FTC showed concern for transparency. W3 Innovations is a mobile application development company with approximately forty applications that target children.[35] In many instances, W3 Innovations failed to post a policy detailing information collected from children, use of such information, disclosure practices, and other required content under COPPA.[36] As a result, the FTC charged the company with a violation of COPPA.[37]

26. *Id.* ¶¶ 32–33.
27. *Id.* ¶¶ 43–47.
28. *Id.* ¶¶ 50–53.
29. *Id.* ¶¶ 56–63.
30. Complaint at ¶ 10, United States v. Godwin, No. 11-cv-03846-JOF (N.D. Ga. Nov. 8, 2011), *available at* http://www.ftc.gov/os/caselist/1123033/111108skidekidscmpt.pdf.
31. *Id.* ¶¶ 11, 17–18.
32. *Id.* ¶¶ 14–16.
33. *Id.* ¶ 19.
34. *Id.* ¶¶ 20–25.
35. Complaint ¶ 12, United States v. W3 Innovations, LLC, CV11-03958 (N.D. Cal. Aug. 12, 2011), *available at* http://www.ftc.gov/os/caselist/1023251/110815w3cmpt.pdf. Justin Maples, the owner of 56 percent of W3 Innovations, is also a defendant.
36. *Id.* ¶¶ 13–25.
37. *Id.* ¶¶ 26–27.

Credit Resellers

In its actions against credit resellers, the FTC showed concern for privacy by design. The FTC brought actions against three credit resellers—SettlementOne Credit Corporation, ACRAnet, Inc., and Fajilan and Associates d/b/a Statewide Credit Services—for failing to take reasonable information security measures to protect consumer data.[38] As a result of this failure, hackers accessed more than 1,800 credit reports without authorization.[39]

Teletrack

Teletrack is a consumer reporting agency that assembles and sells consumer credit reports to third parties.[40] Teletrack has marketing lists that contain the names of consumers and information that may determine a consumer's eligibility for credit.[41] The Fair Credit Reporting Act ("FCRA") has enumerated purposes for which a consumer reporting agency may furnish consumer reports to third parties.[42] Teletrack sold consumer reports for marketing, a purpose not enumerated in the FCRA.[43] As a result, the FTC charged Teletrack with a violation of the FCRA and section 5 of the FTC Act.[44]

FTC Reports

Protecting Consumer Privacy in an Era of Rapid Change

In March 2012, the FTC released its final privacy framework ("Final Report") to update and clarify the preliminary report released in 2010.[45] The Final Report is broken down into three sections that address the background leading to the Final Report and the main themes from commentators on the preliminary report, the privacy framework established in the Final Report, and the policy initiatives the FTC will undertake to assist with the implementation of the final privacy framework.[46]

The final framework applies to most companies, but not those that collect only "non-sensitive data from fewer than 5,000 consumers a year provided they do not share the data with third parties."[47] The Final Report urges companies to adopt the following best practices to protect consumers' private information:

38. Complaint ¶ 8, *In re* SettlementOne Credit Corp., No. 082-3208, 2011 WL 3726287 (FTC Aug. 27, 2011).
39. *Id.* ¶ 10.
40. Complaint ¶ 8, United States v. Teletrack, Inc., No. 1:11-cv-2060 (N.D. Ga. June 24, 2011), *available at* http://www.ftc.gov/os/caselist/1023075/110627teletrackcmpt.pdf.
41. *Id.* ¶¶ 9–13.
42. *Id.* ¶ 14.
43. *Id.*
44. *Id.* ¶¶ 15–17.
45. Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (Mar. 2012) [hereinafter Protecting Consumer Privacy], *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.
46. *Id.*
47. *Id.* at 15.

privacy by design, simplified choice for businesses and consumers, and greater transparency for information collection and use practices.[48] The Final Report explains that data is not "reasonably linkable" when a company: "(1) takes reasonable measures to ensure that data is de-identified; (2) publicly commits not to try to reidentify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data."[49] Although the Final Report does not serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC, it provides an idea of what might be considered for future privacy legislation and sound guidelines for companies to follow when considering privacy.[50]

The FTC describes best practices for privacy through a series of final principles in the report in three areas: privacy by design, consumer choice, and transparency.

In the Final Report, the FTC elaborated on the privacy by design principle to promote consumer privacy throughout organizations and at every stage of development of products and services.[51] The FTC further encouraged companies to incorporate into their practices certain privacy protections, such as data security, reasonable collection limits, sound retention and disposal practices, data accuracy, and comprehensive data management.[52]

To promote simplified consumer choice, the FTC stressed context and relationship.[53] In line with this principle, companies should offer choice at a time and in a context in which the consumer is making a decision about his or her data.[54] The FTC stated that companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes.[55]

The FTC emphasized that companies should increase the transparency of their data practices through making privacy notices clearer, shorter, and more standardized so consumers may better understand privacy practices.[56] Companies may also increase transparency through providing consumers with reasonable access to the data they maintain and should expand efforts to educate consumers about commercial data privacy practices.[57]

In addition to recommending best practices, the FTC plans to assist with the implementation of self-regulatory principles in five areas: (1) Do Not Track; (2) Mobile; (3) Data Brokers; (4) Large Platform Providers; and (5) Promoting Enforceable Self-Regulatory Codes.[58]

48. *Id.* at i.
49. *Id.* at iv.
50. *Id.* at iii.
51. *Id.* at 22.
52. *Id.* at 23–29.
53. *Id.* at 36–39.
54. *Id.* at 48–50.
55. *Id.* at 60.
56. *Id.* at 61–64.
57. *Id.* at 71–72.
58. *Id.* at 72–73.

Mobile Apps for Kids: Current Privacy Disclosures are Disappointing

In addition to the Final Report, the FTC released a staff report entitled *Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing* in February 2012.[59] To study mobile application disclosures, the FTC examined the disclosure pages of 960 mobile applications targeted to children.[60] In this report, the FTC concluded that disclosures were inadequate because parents could not usually determine before downloading an application whether the application posed risks associated with the collection, use, and sharing of children's personal information.[61] The FTC called upon all stakeholders in the mobile app ecosystem to do more to inform parents about the apps downloaded for their children.[62] The FTC recommended that app developers provide information via short disclosures or icons.[63] The FTC also called on app stores to provide basic architecture for the provision of such information, such as standardized icons to signal features, in addition to increasing enforcement of preexisting disclosure requirements for apps.[64] In sum, the FTC found that the current disclosures for children's mobile applications could be improved with the help of different stakeholders to provide greater notice, choice, and transparency to consumers.[65]

Conclusion

In the past year, the FTC has confirmed its commitment to privacy through increasing enforcement and releasing reports. In addition, the FTC has gone beyond its previous promise to protect consumer privacy through added initiatives.

To promote children's privacy, the FTC suggested revising COPPA to add provisions and update definitions, notice, parental consent, confidentiality, and security requirements, and safe harbor programs.[66] To address FCRA-related privacy issues, the FTC warned marketers with mobile background screening apps of possible violations.[67]

Internationally, the FTC has also taken steps to maintain consistency with the 2004 Asia-Pacific Economic Cooperation Privacy Framework and is in the process of formulating a privacy framework agreement with the European Union.[68] Domestically, the FTC is working with other agencies on privacy and calls upon

59. Fed. Trade Comm'n, Mobile Apps for Kids: Current Privacy Disclosures are Disappointing (Feb. 2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.
60. *Id.* at 4–5.
61. *Id.* at 17.
62. *Id.*
63. *Id.* at 3.
64. *Id.*
65. *Id.* at 17.
66. Children's Online Privacy Protection Rule, 76 Fed. Reg. 59804 (proposed Sept. 27, 2011) (to be codified at 16 C.F.R. pt. 312).
67. Press Release, Fed. Trade Comm'n, FTC Warns Marketers that Mobile Apps May Violate Fair Credit Reporting Act (Feb. 7, 2012), *available at* http://www.ftc.gov/opa/2012/02/mobileapps.shtm.
68. Protecting Consumer Privacy, *supra* note 45, at 10.

Congress to consider enacting baseline privacy legislation.[69] To explore further areas that may concern privacy, the FTC has held or plans to hold forums on facial recognition technology, child identity theft, and location-based services.[70]

In sum, the FTC has laid out a solid framework for companies to follow to maintain consumer privacy and has kept its promise to increase enforcement actions for privacy.

69. *Id.* at 72.
70. *Id.* at A-1 to A-8.

L'Embarras du Choix: A Year of Developments in the Laws Affecting Remittance Transfers, Credit Cards, and Certain Prepaid Cards

*By Sarah Jane Hughes**

I. Introduction

Following Richard Cordray's appointment as the first Director of the Bureau of Consumer Financial Protection ("CFPB"),[1] the CFPB began to exercise the authority given to it by Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ("Dodd-Frank Act").[2] Its recent final and proposed rules and additional notices of proposed rulemaking affecting e-payments and credit services are among the most significant e-payments developments since June 2011. However, they were not the only significant e-payments developments in the past year. Accordingly, this survey also covers selected developments from two other federal agencies, the Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") and the Board of Governors of the Federal Reserve System ("the Board"), state-law developments related to remittance payments, and decisions from courts in the United States and the European Union since last year's survey.[3]

Part II of this survey covers the CFPB's February 2012 final "remittance transfer" amendments to Regulation E,[4] which implement the Electronic Fund

* Sarah Jane Hughes is the University Scholar and Fellow in Commercial Law at Indiana University's Maurer School of Law in Bloomington, Indiana, and a survey contributor since 2006. She is a graduate of Mount Holyoke College and the University of Washington School of Law. Professor Hughes thanks Amber Benson, Maurer School Class of 2012, and Eli Roberts, Maurer School Class of 2013, for research assistance; despite such talented help, she takes responsibility for all errors.

1. Christie L. Grymes, *Cordray Gets Recess Appointment to Head CFPB*, Consumer Fin. L. Blog (Jan. 5, 2012), http://www.consumerfinancelawblog.com/2012/01/articles/consumer-financial-protection/cordray-gets-recess-appointment-to-head-cfpb/.

2. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, tit. X, 124 Stat. 1376, 1955–2113 (2010); *see* 12 U.S.C. § 5581 (Supp. IV 2010); 15 U.S.C. § 1604(a) (2006 & Supp. IV 2010); Designated Transfer Date, 75 Fed. Reg. 57252, 57252 (Sept. 20, 2010) (designating transfer of certain authorities to the new Bureau of Consumer Financial Protection on July 21, 2011).

3. For discussion of electronic payments and financial services developments from June 1, 2010, to June 1, 2011, see Sarah Jane Hughes, *Developments in the Laws Governing Electronic Payments*, 67 Bus. Law. 259 (2011) [hereinafter *2011 Electronic Payments Developments*].

4. Electronic Fund Transfers, 77 Fed. Reg. 6194 (Feb. 7, 2012) (to be codified at 12 C.F.R. pt. 1005) [hereinafter Final Regulation E Remittance Transfer Amendments]. The Final Regulation E Remittance Transfer Amendments will take effect on February 7, 2013. *Id.* at 6194.

Transfer Act ("EFTA"),[5] and several subsequent actions to close a regulatory gap those amendments created for consumers and certain remittance providers taken or to be taken by the Board to amend Regulation J,[6] the American Law Institute ("ALI") and Uniform Law Commission,[7] and New York State.[8]

Part III focuses on credit card fee regulations in the United States and the European Union, particularly a 2011 preliminary injunction granted to First Premier Bank against implementation of the Federal Reserve Board 2010 Credit CARD Act first-year fee regulations,[9] and the May 24, 2012 decision by the General Court in *MasterCard, Inc. v. European Commission*.[10]

Part IV focuses on three of many developments in the laws affecting "gift cards" and other "stored-value" or "prepaid" products. These include FinCEN's July 2011 amendments to Bank Secrecy Act ("BSA") regulations to reach "prepaid" cards,[11] the January 5, 2012 decision by the United States Court of Appeals for the Third Circuit in *New Jersey Retail Merchants Ass'n v. Sidamon-Eristoff*,[12] and the CFPB's May 2012 notice of proposed rulemaking on reloadable prepaid cards.[13]

II. The CFPB Adopts Remittance Transfer Regulations and Exposes a Regulatory Gap Affecting Certain Fund Transfers

The federal EFTA[14] and its implementing regulation (Electronic Fund Transfers, commonly known as Regulation E) apply to electronic fund transfers if the

5. Pub. L. No. 95-630, 92 Stat. 3728 (1978) (codified at 15 U.S.C. §§ 1693–1693r (2006 & Supp. IV 2010)).

6. Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire: Elimination of "As-of Adjustments" and Other Clarifications, 77 Fed. Reg. 21854, 21856 (Apr. 12, 2012) (to be codified at 12 C.F.R. pt. 210) [hereinafter Reg. J Final Amendments].

7. For a summary of this issue and the action proposed to the membership of the American Law Institute and Uniform Law Commissioners, see Memorandum from Lance Liebman & John Sebert to Members of the Am. Law Inst. & Unif. Law Comm'n Exec. Comm., Proposed Amendment to UCC Section 4A-108 (May 4, 2012) [hereinafter Liebman-Sebert May 2012 Memorandum], *available at* www.ali.org/doc/UCC 4a-108.pdf. The members of the ALI approved a new version of U.C.C. § 4A-108 at the ALI's Annual Meeting. *See 89th Annual Meeting Updates: UCC Article 4A*, Am. L. Inst. (May 23, 2012, 10:59 AM), http://2012am.ali.org/updates.cfm [hereinafter ALI UCC Article 4A Update].

8. S. 07493A, 2011 Gen. Assemb., Reg. Sess. (N.Y. 2012) [hereinafter NY UCC Article 4A Proposed Amendment], *available at* http://assembly.state.ny.us/leg/?default_fld=&bn=S07493&term=2011&Summary=Y&Actions=Y&Text=Y&Votes=Y.

9. First Premier Bank v. CFPB, 819 F. Supp. 2d 906, 923 (D.S.D. 2011) (enjoining implementation of the Board's expanded 2011 version of 12 C.F.R. § 1026.52(a) on the ground that the Board's interpretation of the Credit CARD Act was not entitled to deference).

10. Case T-111/08, 5 C.M.L.R. 5 (2012).

11. Bank Secrecy Act Regulations—Definitions and Other Regulations Relating to Prepaid Access, 76 Fed. Reg. 45403 (July 29, 2011) (to be codified at 31 C.F.R. §§ 1010, 1022) [hereinafter FinCEN's Prepaid Access Regulation Amendments]. The rule's effective date was set for September 27, 2011, with a compliance date of January 29, 2012. *Id.* at 45403.

12. 669 F.3d 374 (3d Cir. 2012).

13. Electronic Fund Transfers, 77 Fed. Reg. 30923 (May 24, 2012) (to be codified at 12 C.F.R. pt. 1005) [hereinafter Regulation E Reloadable Prepaid Cards ANPR].

14. Pub. L. No. 95-630, 92 Stat. 3728 (1978) (codified at 15 U.S.C. §§ 1693–1693r (2006 & Supp. IV 2010)).

medium of communication is electronic, the person initiating the instruction is a consumer, and the instruction is to debit or credit an account the consumer holds with the financial institution receiving the instruction.[15] Section 1073 of the Dodd-Frank Act mandated amendments to Regulation E to provide consumer protection rules for remittance transfers sent by consumers in the United States to beneficiaries in other countries.[16] The consumer protection rules added time-limited transfer-cancellation rights, requirements for the investigation by providers of alleged errors, and remedies for errors.[17]

Dodd-Frank Act section 1073's additions of "remittance transfer" provisions to the EFTA and the CFPB's Final Regulation E Remittance Transfer Amendments will create, as of their effective date in 2013, a regulatory gap among the EFTA, Article 4A of the Uniform Commercial Code, Regulation J, and Article 4A's incorporation in system rules and contracts such as those governing CHIPS.[18] This gap, as well as steps to close the gap already underway, are described below.

A. The CFPB's Regulation E Amendments Will Govern Cross-Border Remittance Transfers in 2013

Both the Board and the CFPB participated in the Regulation E amendments to implement the Dodd-Frank Act's section 1073. The Board issued the pertinent Notice of Proposed Rulemaking in 2011,[19] and the CFPB, which assumed enforcement and rulemaking authority for the EFTA on July 21, 2011,[20] issued the Final Regulation E Remittance Transfer Amendments.[21]

The CFPB's Final Regulation E Remittance Transfer Amendments will apply Regulation E's subpart A to any person, not only financial institutions, and subpart B only to remittance transfer providers.[22] Regulation E will govern all cross-border "remittance transfers," which are defined as the "electronic transfer of funds," if the remittance transfer is made in the normal course of the provider's business.[23] A transfer is characterized as a "remittance transfer" even when the consumer sender does not own an account with the remittance transfer provider.[24] For purposes of defining "remittance transfer," it is irrelevant whether

15. 12 C.F.R. § 1005.3(a) (2012).
16. 15 U.S.C. § 1693o-1 (Supp. IV 2010).
17. *Id.*
18. *See* Reg. J Final Amendments, *supra* note 6, at 21856.
19. Electronic Fund Transfers, 76 Fed. Reg. 29902 (proposed May 23, 2011) (to be codified at 12 C.F.R. pt. 205) [hereinafter Proposed Board Regulation E Remittance Transfer Amendments].
20. Designated Transfer Date, 75 Fed. Reg. 57252, 57252 (Sept. 20, 2010); Dodd-Frank Act §§ 1025(b), 1061, 1100A, 12 U.S.C. §§ 5515(b), 5581, 1604(b) (Supp. IV 2010).
21. Final Regulation E Remittance Transfer Amendments, *supra* note 4. Together with the Final Regulation E Remittance Transfer Amendments, the CFPB issued a separate proposed rule to obtain additional comments on the Final Amendments' coverage and preauthorized remittance transfers. Electronic Fund Transfers, 77 Fed. Reg. 6310 (proposed Feb. 7, 2012) (to be codified at 12 C.F.R. pt. 1005). This survey does not discuss the 2012 proposal.
22. Final Regulation E Remittance Transfer Amendments, *supra* note 4, at 6285.
23. 12 C.F.R. § 1005.30(e), (f) (2012).
24. *Id.*

the transaction is also classified as an "electronic fund transfer," as defined in 12 C.F.R. § 1005.3(b), which is a transfer where the consumer's instruction was by electronic means.[25] The new rules will not govern transactions of $15 or less, but will govern "preauthorized" transfers that "recur at substantially regular intervals."[26]

The Final Regulation E Remittance Transfer Amendments require both pre-payment, pre-transfer disclosures and post-payment receipt disclosures. The pre-payment, pre-transfer disclosures include basic terms of the transfer, specifically a disclosure that shows the rate of currency exchange, transfer fees and taxes to be collected from the sender, the amount of currency to be delivered to the recipient at the local exchange rate, the total cost of the remittance transfer, and the total the recipient will receive.[27] Reasonably accurate estimates may be substituted if the provider is a bank or credit union or if the remittance is to be sent to certain countries.[28]

The payment receipt must include the recipient's (beneficiary's) name and telephone number (if the sender has provided it), the date that funds will be available to the recipient, a statement about the sender's error resolution and cancellation rights using Model Form A-37 in Appendix A, the provider's name, telephone number(s), and website, and full contact information for the state agency that regulates license remittance providers and the CFPB.[29] It also must explain both the sender's error resolution rights,[30] including any procedures to be followed, and the provider's liability for sending the wrong sum of money to the designated recipient or delivering the funds to the wrong recipient.[31] Remedies for transfer errors include disbursing the proper amount of funds available to the designated recipient, making a sum appropriate to resolving the error available to the sender, or refunding any fees or taxes, if not prohibited by domestic or foreign law, to the sender.[32]

The scope of the sender's error resolution rights depends on the totality of the transfer. For example, if an alleged error involves an extension of credit, Regulation Z's error resolution procedures will govern regardless of the identity of the remittance transfer provider.[33] Alleged unauthorized transfers are to be resolved pursuant to Regulation E's basic rules, which are now codified in §§ 1005.6 and 1005.11, with respect to the account-holding institution.[34]

25. *Id.*
26. *See id.* § 1005.30(e)(2), (d).
27. *Id.* § 1005.30(b)(i)–(vii).
28. *Id.* § 1005.32.
29. *Id.* § 1005.31(b)(2). The explanation of the right to cancel must meet the requirements of § 1005.36(c) if the transfer is scheduled for at least three days before the actual transfer is to take place. *Id.* § 1005.32(b)(iv).
30. *Id.* § 1005.31(b)(2)(iv). Senders have up to 180 days to report errors and request resolution of errors. *Id.* § 1005.33(b)(i).
31. *Id.* § 1005.33.
32. *Id.* § 1005.33(c)(2).
33. *Id.* § 1005.33(f)(2).
34. *Id.* § 1005.33(f)(3).

The Final Regulation E Remittance Transfer Amendments drew criticism from banks and non-bank providers of remittance services[35] and praise from consumer groups.[36] Some bank industry groups called for an extension of the mandatory compliance date and for substantive changes to the rule.[37]

B. The Board Amends Regulation J to Protect Fedwire Participants

Prior to the CFPB's amendments to Regulation E promulgated in early 2012, the Board had already proposed amendments to Regulation J's Fedwire provisions.[38] On April 12, 2012, the Board amended Regulation J so that its subpart B would continue to apply to Fedwire fund transfers even if the fund transfers also would qualify as "remittance transfers."[39] The Board explained that its Regulation J amendments were "intended to ensure that the provisions of Regulation J, and therefore Article 4A of the [U.C.C.], apply to all Fedwire funds transfers, except to the extent that section 919 of the EFTA and rules established thereunder apply."[40] The Board also acknowledged the need for the U.C.C. Article 4A amendment described next in this survey to remedy the gap for non-Fedwire transactions.[41]

C. The American Law Institute Approves U.C.C. Article 4A Amendments to Protect Non-Fedwire Funds Transfer Participants

As the Board proposed amendments to Regulation J, it also suggested amendments to U.C.C. § 4A-108, which explains the relationship of U.C.C. Article 4A to the EFTA.[42] On May 23, 2012, the ALI approved amendments to U.C.C. § 4A-108, developed in cooperation with the Uniform Law Commissioners, to resolve the regulatory gap that will arise once the Final Regulation E Remittance Transfer Amendments go into effect in 2013.[43]

35. *See News Now: CU Remittance Concerns Aired at D.C. Symposium*, Credit Union Nat'l Ass'n (Apr. 20, 2012), http://www.cuna.org/newsnow/12/wash041912-3.html; *see also* Becky Nelson, *CFPB Updates Remittance Rules*, CFPB J. (Feb. 8, 2012), http://cfpbjournal.com/issue/cfpb-journal/article/cfpb-updates-remittance-rules.

36. *See* Press Release, Consumers Union, CFPB Announces Plan to Develop Rules Requiring Better Prepaid Card Fee Disclosure and Other Protections for Consumers (May 23, 2012), *available at* http://www.consumersunion.org/pub/core_financial_services/018415.html; Anthony Giorgianni, *Federal Rules Offer New Money-Transfer Protections*, ConsumerReports.org (Mar. 15, 2012), http://news.consumerreports.org/money/2012/03/send-money-abroad-remittances-regulations.html.

37. *See* Letter from James Aramanda & Paul Saltzman, Clearing House Ass'n, L.L.C., to Richard Cordray, Dir., Bureau of Consumer Fin. Prot. (Apr. 27, 2012) [hereinafter Clearing House Letter], *available at* http://www.theclearinghouse.org/index.html?f=073844.

38. Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire: Elimination of "As-of Adjustments" and Other Clarifications, 76 Fed. Reg. 64259 (proposed Oct. 18, 2011) (to be codified at 12 C.F.R. § 210.25) [hereinafter Proposed Reg. J Amendments].

39. Reg. J Final Amendments, *supra* note 6, at 21854–57 (to be codified at 12 C.F.R. pt. 210.25).

40. *Id.* at 21856.

41. *Id.*

42. Reg. J Final Amendments, *supra* note 6, at 21856.

43. *See* ALI UCC Article 4A Update, *supra* note 7.

Without the states' timely enactment of the proposed U.C.C. Article 4A amendments, some transfers no longer would be governed by either Article 4A or the EFTA. This result would be the case for funds transfers initiated by remittance transfers even if the remittance transfer would not also qualify as an "electronic fund transfer," as the EFTA defines that term.[44] Thus, cross-border remittance transfers subject to the Final Regulation E Remittance Transfer Amendments and made in person or in writing, as opposed to by electronic means, would not qualify as "electronic fund transfers" under the EFTA and Regulation E.[45] As a result, those transfers would no longer be covered by Article 4A's rules that govern parties' rights and responsibilities.[46] Accordingly, providers of cross-border "remittance transfers" that are not "electronic fund transfers" would have to execute transaction-specific contracts or renegotiate their bilateral contracts with their transfer system counterparts to cover rights and responsibilities that U.C.C. Article 4A already addresses.[47]

The proposed U.C.C. § 4A-108 solution clarifies that Article 4A would govern issues affecting funds transfers that are "remittance transfers" but not "electronic fund transfers," as defined by 15 U.S.C. § 1693o-1 and Regulation E, an exception to the remittance transfer provisions of the EFTA and Regulation E.[48] It also provides that the provisions of the EFTA govern in the event of a conflict to the extent of the inconsistency.[49] With the ALI's approval, the proposed amendment became ripe for action by the Uniform Law Commissioners and state legislatures.

D. New York State Considers Its Own U.C.C. Article 4A Amendments

With modest textual differences from the ALI-approved amendments discussed in the preceding subpart, New York's State Assembly is considering Senate Bill No. 07493 to amend New York's section 4-A-108, to exclude consumer transactions governed by federal law from New York's section 4-A-108.[50] If other states enact the ALI-approved amendments, Article 4A will not be as uniform as it might have been. At this time, Senate Bill No. 07493 has not been signed into law. Whether New York will amend its version to conform to versions adopted by other states, and the degree to which states follow New York's lead or follow the ALI's recommended version, remains an open question.

III. The United States and the European Union Tackle Credit Card Fees (Again)

This part of this survey covers three significant developments since June 2011 relating to credit card fees in the United States and the European Union.

44. *Id.*; *see also* Liebman-Sebert May 2012 Memorandum, *supra* note 7, at 1.
45. Liebman-Sebert May 2012 Memorandum, *supra* note 7, at 1.
46. *Id.* For additional information on the regulatory gap, see Clearing House Letter, *supra* note 37, at 4, 11.
47. Liebman-Sebert May 2012 Memorandum, *supra* note 7, at 5.
48. *Id.*
49. *Id.*
50. NY UCC Article 4A Proposed Amendment, *supra* note 8.

A. The CFPB Adjusts First-Year Credit Card Fee Regulations After Losing a Challenge

The Credit CARD Act of 2009 added to the Truth in Lending Act new requirements for open-end consumer credit transactions, which include a prohibition on collection of any fees ("other than any late fee, over-the-limit fee, or fee for a payment returned for insufficient funds") from the available credit of the account if the terms of the open-end plan require the payment of fees during the first year that amount to more than 25 percent of the authorized credit of the account.[51] These new requirements have prompted multiple actions by the Board and CFPB, including a revision following a successful action to enjoin enforcement of one of the Board's actions, all of which are described below.

The Board had promulgated amendments to Regulation Z to implement the Credit CARD Act requirements in February 2010.[52] Then, in April 2011, it promulgated expanded requirements.[53] On September 23, 2011, a federal district court in South Dakota granted a preliminary injunction against the implementation of the expanded pre-account-opening fee limitations in the 2011 Credit Card Fee Rule.[54]

As a result of this preliminary injunction and following the transfer of authority for the Credit CARD Act to the CFPB described above,[55] on April 12, 2012, the CFPB proposed amendments to the 2011 Credit Card Fee Rule.[56] The 2012 proposed amendments exempt fees to be paid prior to account opening from the limitation in the 2011 Credit Card Fee Rule as codified at 12 C.F.R. § 1026.52(a).[57]

B. MasterCard Loses Its Challenge to the European Commission's 2007 Ruling on Cross-Border Credit Card Interchange Fees

On May 24, 2012, the General Court confirmed a December 2007 European Commission ban[58] on charges by MasterCard and two subsidiaries—MasterCard

51. 15 U.S.C. § 1637(n)(1) (Supp. III 2009).

52. Truth in Lending, 75 Fed. Reg. 7658 (Feb. 22, 2010) (to be codified at 12 C.F.R. § 1026.52(a)).

53. Truth in Lending, 76 Fed. Reg. 22948 (Apr. 25, 2011) (to be codified at 12 C.F.R. § 1026.52(a)) [hereinafter 2011 Credit Card Fee Rule]. For a thorough discussion of the Federal Reserve Board's other Credit CARD Act regulation clarifications in 2011, including comments on section 226.52(a) (now recodified in section 1026.52(a)), see Obrea Poindexter, *Summary of 2011 Credit CARD Act Clarifications*, 67 Bus. Law. 663 (2012).

54. First Premier Bank v. CFPB, 819 F. Supp. 2d 906, 923 (S.D. 2011).

55. Designated Transfer Date, *supra* note 2, at 57252 (designating transfer of certain authorities to the new Bureau of Consumer Financial Protection on July 21, 2011).

56. Truth in Lending, 77 Fed. Reg. 21875 (proposed Apr. 12, 2012) (to be codified at 12 C.F.R. pt. 1026).

57. *Id.* at 21876.

58. The 2007 decision by the European Commission on appeal was prompted by complaints from the British Retail Consortium and EuroCommerce AISBL against the predecessor of MasterCard Europe. Summary of Commission Decision Relating to a Proceeding Under Article 81 of the EC Treaty and Article 53 of the EEA Agreement of 19 Dec. 2007, 2009 O.J. (C 264) 8.

International, Inc. and MasterCard Europe—for cross-border retail transactions on the ground that they breached EU antitrust laws.[59] The 2007 ban applied EU antitrust laws to a class of interchange fees that the parties defined as "multilateral fallback interchange fees which apply within the EEA or Euro area, that is excluding interchange fees agreed bilaterally between issuing and acquiring banks or interchange fees set collectively at [the] national level ('MIF')."[60] Key findings in the 2007 decision were that: (1) (a) MasterCard was an "association of undertakings" and (b) the MIF "led to a restriction of price competition between acquiring banks to the detriment of merchants and their customers"; (2) the MIF "aggravated" the effects of restrictions on competition in the issuing market and the interchange systems market; and (3) acquiring banks had no incentive to exert downward pressure on MIF pricing and, concurrently, merchants had no ability to "constrain the level of the MIF."[61] MasterCard had applied for annulment of the 2007 ban, or of portions of the ban, to the General Court.[62]

The General Court rejected the application to annul the 2007 decision and dismissed MasterCard's action.[63] MasterCard promptly announced its intention to appeal the 2012 decision.[64]

IV. U.S. Regulators and Courts Take Actions on Prepaid Cards

This part of the survey discusses three significant developments relating to prepaid cards or access since June 2011.

A. FinCEN Amends Anti-Money Laundering Regulations to Cover Prepaid Products

FinCEN's 2011 Prepaid Access Rule,[65] which amends its prior Money Services Business Anti-Money Laundering ("AML") regulations,[66] is in response to section 503 of the Credit CARD Act.[67] The Credit CARD Act mandated Bank Secrecy Act[68]

59. Case T-111/08, MasterCard, Inc. v. Eur. Comm'n, 5 C.M.L.R. 5, ¶¶ 1, 16–20 (2012).
60. *Id.* ¶ 20 (referring to recital 118 of the 2007 ban).
61. *Id.* ¶¶ 24, 28 (referring to recitals 410, 411, and 522 of the 2007 ban), ¶¶ 31–33.
62. *Id.* ¶¶ 1, 45.
63. *Id.* ¶ 332.
64. *MasterCard Says to Appeal EU Court Fees Ruling*, Reuters (May 24, 2012), http://www.reuters.com/article/2012/05/24/eu-mastercard-appeal-idUSB5E8GN00D20120524 (quoting MasterCard President Javier Perez).
65. FinCEN's Prepaid Access Regulation Amendments, *supra* note 11, at 45403.
66. Amendment to the Bank Secrecy Act Regulations—Definitions Relating to, and Registration of, Money Services Businesses, 64 Fed. Reg. 45438 (Aug. 20, 1999) (defining original AML obligations for issuers, sellers, and redeemers of stored value). FinCEN's regulations generally governing money services businesses are codified at 31 C.F.R. §§ 1022.210, 1010.311, 1022.320, 1010.415 & 1022.410 (2012).
67. Credit CARD Act of 2009, Pub. L. No. 111-24, § 503(a), (c), 123 Stat. 1734, 1756 (codified at 31 U.S.C. § 5311 (2006 & Supp. IV 2010)).
68. Pub. L. No. 91-508, tits. I, II, 84 Stat. 1114, 1114–24 (1970) (codified as amended at 12 U.S.C. §§ 1829b, 1951–1959 & 31 U.S.C. §§ 5311–5314, 5316–5332 (2006 & Supp. IV 2010)).

regulations for the "sale, issuance, redemption, or international transport of stored value, including stored value cards."[69] "Prepaid access" products include devices such as "plastic cards, mobile phones, electronic serial numbers, key fobs and/or other mechanisms that provide a portal to funds that have been paid for in advance and are retrievable or transferable."[70]

FinCEN's 2011 Prepaid Access Rule adopts a "targeted approach to regulating sellers of prepaid access products" and focuses "on the sale of prepaid access products whose inherent features or high dollar amounts pose heightened money laundering risks."[71] Consistent with the targeted-approach philosophy, the rule exempts categories of products from its coverage.[72]

Issuers, marketers, and sellers in a multi-level prepaid access program must designate a single entity to serve as the "provider" that will maintain transactional information and provide the information to FinCEN on request.[73] "Sellers" of prepaid access products[74] must (1) maintain anti-money laundering programs, (2) file Suspicious Activity Reports, and (3) comply with other recordkeeping requirements governing customer identifying information.[75] Commentators hailed this requirement for making the rule "far more workable" than the proposed rule.[76]

B. The Third Circuit Upholds Limitations on New Jersey's 2010 "Gift Card" Escheat Amendments

Last year's survey reported on a federal district court's injunction against New Jersey's 2010 amendments to its escheat statutes to include certain "gift cards."[77] The district court had enjoined two aspects of the amendments, *viz.*, the state's "place-of-purchase" presumption for its jurisdictional claim to escheat priority and the law's retroactive application for cards sold prior to its original effective date of July 1, 2010.[78] The district court did not enjoin the amendment's "data collection" provision requiring the collection of the

69. Credit CARD Act of 2009, Pub. L. No. 111-24, § 503(a), 123 Stat. 1734, 1756 (codified at 31 U.S.C. § 5311 (2006 & Supp. IV 2010)).

70. 31 C.F.R. § 1010.100(ww) (2012) (definition of "prepaid access"); FinCEN's Prepaid Access Regulation Amendments, *supra* note 11, at 45406. For more information, see Press Release, Fin. Crimes Enforcement Network, FinCEN Issues Prepaid Access Final Rule Balancing the Needs of Law Enforcement and Industry (July 26, 2011), *available at* http://www.fincen.gov/news_room/nr/html/20110726b.html.

71. 31 C.F.R. § 1010.100(ww).

72. *Id.* § 1010.100(ff)(4)(iii)(A)–(D).

73. *Id.* §§ 1010.100(ff)(4), 1022.420.

74. For the definition of "seller of prepaid access products," see *id.* § 1010.100(ff)(7).

75. *Id.* § 1022.210.

76. *See* Press Release, Ballard Spahr LLP, FinCEN Adopts Final Rule on Prepaid Access (Aug. 2, 2011), *available at* http://www.ball.ardspahr.com/alertspublications/legalalerts/2011-08-02_fincen_adopts_final_rule_on_prepaid_access.aspx.

77. *2011 Electronic Payments Developments*, *supra* note 3, at 277–78.

78. Am. Express Travel Related Servs. Co. v. Sidamon-Eristoff, 755 F. Supp. 2d 556, 563 (D.N.J. 2010).

card purchasers' names and addresses and the maintenance of the purchasers' zip codes.[79]

In a January 5, 2012 decision, the United States Court of Appeals for the Third Circuit in *New Jersey Retail Merchants Ass'n v. Sidamon-Eristoff* affirmed the district court's rulings on all three issues.[80] Thus, following the decision, most sellers of cards in New Jersey must collect the names, addresses, and zip codes of gift card purchasers, and issuers of cards face a two-year period after a card's sale before the funds remaining on the card will escheat.[81] Following the Third Circuit's decision, news media reported that retailers were withdrawing "gift cards" from the New Jersey markets in response to the 2010 statute.[82]

C. The CFPB Looks at Regulating General Purpose Reloadable Prepaid Cards

The CFPB issued both an Advance Notice of Proposed Rulemaking on Prepaid Cards[83] and held a field hearing on prepaid cards on May 23, 2012.[84] The ANPR seeks information on ten questions pertaining to general purpose reloadable prepaid cards and other devices, such as key fobs and cell phone applications, which allow consumer access to a financial account.[85] The ANPR does not

79. *Id.* at 623. The court noted that its "opinion is limited to the challenge brought against 2010 N.J. Laws Chapter 25 . . . with respect to stored value cards." *Id.* at 623 n.1. Chapter 25's additions to the New Jersey escheat statute are codified in various subsections of N.J. Stat. Ann. § 46:30B (West 2003 & Supp. 2011).

80. 669 F.3d 374 (3d Cir. 2012).

81. N.J. Stat. Ann. § 46:30B-42.1 (West 2003 & Supp. 2011). Responding to the plaintiffs' arguments that the Credit CARD Act's provision on card expiry preempted New Jersey's new two-year escheat schedule, the Third Circuit ruled that New Jersey's 2010 amendments provided more protection for consumers and, accordingly, the Credit CARD Act did not preempt the New Jersey statute. *N.J. Retail Merchs. Ass'n*, 669 F.3d at 389. For a superb discussion of escheat and e-payments generally, see Anita Ramasastry, *State Escheat Statutes and Possible Treatment of Stored Value, Electronic Currency, and Other New Payment Mechanisms*, 57 Bus. Law. 475 (2001).

82. *See, e.g.*, Joel Rose, *New Jersey Law Causes Companies to Pull Gift Cards*, NPR.org (Apr. 9, 2012), http://www.npr.org/2012/04/09/150268403/retailers-may-stop-selling-gift-cards; *New Gift Card Laws in New Jersey Makes the Offering Less Appealing to Retailers*, RetailPro.com (Apr. 10, 2012), http://www.retailpro.com/community/blog/index.php/2012/04/10/new-gift-card-laws-in-new-jersey-makes-the-offering-less-appealing-to-retailers/.

83. Regulation E Reloadable Prepaid Cards ANPR, *supra* note 13, at 30923. The ANPR's Request for Comment covers regulatory coverage for prepaid products, product fees, and disclosures, product features, and other information on general purpose reloadable prepaid cards, including means of reducing the compliance burdens of prospective regulations. *Id.* at 30925.

84. Press Release, Consumer Fin. Prot. Bureau, Consumer Financial Protection Bureau Considers Rules on Prepaid Cards (May 23, 2012), *available at* http://www.consumerfinance.gov/pressreleases/consumer-financial-protection-bureau-considers-rules-on-prepaid-cards/; *see also* Sharon Kim Schiavetti, *CFPB Holds Field Hearing on General Purpose Reloadable Prepaid Cards*, Consumer Fin. L. Blog (May 24, 2012), http://www.consumerfinancelawblog.com/2012/05/articles/consumer-financial-protection/cfpb-holds-field-hearing-on-general-purpose-reloadable-prepaid-cards/.

85. Regulation E Reloadable Prepaid Cards ANPR, *supra* note 13, at 30923. The questions fall into four groups covering "(A) regulatory coverage of products by some or all of Regulation E, (B) product fees and disclosures, (C) product features, and (D) other information on GPR cards." *Id.* at 30925; *see also* Kristin A. McPartland, *CFPB Issues Advance Notice of Proposed Rulemaking for Prepaid Cards*, Consumer Fin. L. Blog (May 23, 2012), http://www.consumerfinancelawblog.com/2012/05/articles/consumer-financial-protection/cfpb-issues-advance-notice-of-proposed-rulemaking-for-prepaid-cards/.

cover issues with so-called "closed loop" cards, including "debit cards linked to a traditional checking account, non-reloadable cards, payroll cards, electronic benefit transfers (EBTs), or gift cards."[86]

V. Conclusion

Despite efforts to alter the powers and funding of the CFPB that were underway as of the end of June 2011,[87] the CFPB has survived so far and, since Richard Cordray became the Director, has been active. For this survey, there was no new congressional legislation on which to report. But, because of so many other developments, the hardest task by far in writing this survey was not in deciding what to cover; it was more an exercise of *what not to cover*. E-payments law keeps expanding, offering up "l'embarras du choix."

86. Regulation E Reloadable Prepaid Cards ANPR, *supra* note 13, at 30923.
87. *2011 Electronic Payments Developments*, *supra* note 3, at 278.

Electronically Stored Information in Litigation

*By Timothy J. Chorvat and Laura E. Pelanek**

I. Introduction

The law governing the discovery and use of electronically stored information ("ESI") in litigation continues to evolve, through case law spanning *Zubulake*[1] to *Pension Committee*,[2] amendments to the rules of civil procedure,[3] and court-based efforts to address the costs and burden of electronic discovery,[4] in both state and federal systems.[5] That evolution is driven in part by a need for litigation to adapt to new technologies and uses that continue to emerge, such as social media and cloud computing. In this survey, we review the cases that have addressed those new forms of ESI and then look briefly at recent developments in connection with what already can be regarded as more traditional forms of ESI.

II. Social Media: Discovery Requests in a Friend Request World

As social media sites like Facebook and Twitter have come to dominate aspects of many people's lives, those sites have accumulated vast reservoirs of information that lawyers are seeking to tap in litigation. In cases as varied as

* Mr. Chorvat is a partner, and Ms. Pelanek is litigation counsel, in the Chicago office of Jenner & Block LLP.

1. Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC, 230 F.R.D. 290 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC, 216 F.R.D. 280 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004).

2. Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456 (S.D.N.Y. 2010).

3. *See* Fed. R. Civ. P. 16, 26, 33, 34, 37, 45.

4. *See, e.g.*, Seventh Circuit Elec. Discovery Pilot Program Comm., Seventh Circuit Electronic Discovery Pilot Program: Final Report on Phase Two, May 2010–May 2012, at 1 (2012), *available at* http://www.discoverypilot.com/sites/default/files/Phase-Two-Final-Report-Appendix.pdf.

5. For a summary of developments in the federal courts during 2009–2010, see Timothy J. Chorvat & Laura E. Pelanek, *Electronically Stored Information in Litigation*, 66 Bus. Law. 183 (2010). For a summary of the developments in state courts during 2010–2011, see Timothy J. Chorvat & Laura E. Pelanek, *Electronically Stored Information in Litigation*, 67 Bus. Law. 285 (2011).

personal injury actions[6] and commercial litigation,[7] opposing parties are using statements, photographs, and other materials posted online as evidence. Social media services like LinkedIn, Facebook, Twitter, and MySpace permit users to post information for viewing by the public or designated groups, including personal information in profiles, status updates about a user's activities, photographs, and more private direct messages.[8] Upon joining a social media site, a user is encouraged to develop a profile, to provide personal information, and to encourage and accept requests for "connections," "friends," or "followers."[9] Social media sites permit users to protect information to varying degrees through the use of privacy settings,[10] so that adverse parties may not be able to access a user's information outside of discovery.

In recent years, courts have begun to address the discoverability of social media, primarily in connection with Facebook and MySpace postings. Courts tend to allow discovery of social media to proceed when requests are directed to a party after balancing the relevance of the data being sought against privacy and privilege interests.[11]

A. Discovery Requests to Parties Concerning Social Media

One of the first cases to address the discoverability of social media content was *Bass v. Miss Porter's School*, a 2009 federal district court decision from Connecticut, in which the defendant served discovery requests seeking social media data relating to the conduct and pleadings at issue in the action.[12] Based on an *in camera* review, the court concluded that the defendant had demonstrated that the plaintiff's production of social media information had been vastly underinclusive and ordered the plaintiff to provide her complete Facebook profile to the defendant.[13]

Similarly, *EEOC v. Simply Storage, LLC*, a 2010 federal case from Indiana, addressed a request for the production of two claimants' social media profiles and

6. *See, e.g.*, Tompkins v. Detroit Metro. Airport, 278 F.R.D. 387 (E.D. Mich. 2012) (denying motion to compel in a slip-and-fall case); Offenback v. L.M. Bowman, Inc., No. 1:10-CV-1789, 2011 U.S. Dist. LEXIS 66432 (M.D. Pa. June 22, 2011); Zimmerman v. Weis Mkts., Inc., No. CV-09-1535, 2011 Pa. Dist. & Cnty. Dec. LEXIS 187 (Pa. D. & C. May 19, 2011); McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270 (Pa. D. & C. Sept. 9, 2010).

7. *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010).

8. *See, e.g.*, *Basics, Facebook Help Center*, Facebook.com, https://www.facebook.com/help/basics (last visited May 28, 2012); *Profile*, MySpace.com, http://www.myspace.com/help?pm_cmp=ed_footer (last visited May 28, 2012); *Learning Center*, LinkedIn.com, http://learn.linkedin.com/ (last visited May 28, 2012); *Twitter Basics*, Twitter.com, https://support.twitter.com/ (last visited May 28, 2012).

9. *See supra* note 8.

10. *See supra* note 8.

11. *See, e.g.*, *Offenback*, 2011 U.S. Dist. LEXIS 66432, at *10; EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 435–36 (D. Ind. 2010); Bass v. Miss Porter's School, 2009 U.S. Dist. LEXIS 99916, at *1 (D. Conn. 2009); Largent v. Reed, No. 2009-1823 (Pa. D. & C. Nov. 8, 2011); *Zimmerman*, 2011 Pa. Dist. & Cnty. Dec. LEXIS 187, at *9–10; *McMillen*, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *11.

12. *See Bass*, 2009 U.S. Dist. LEXIS 99916, at *1.

13. *Id.* at *4.

communications.[14] The defendant sought that information, contending that the claimants had put their emotional health at issue, because the Facebook and MySpace accounts contained probative information.[15] The court noted that, although social media provides a novel context, basic discovery principles apply.[16] The court explained that social media content is not privileged from discovery merely because the user has deemed it "private," and concluded that privacy concerns can be addressed through a protective order.[17] Citing *Bass*, the court decided that complete production of social media information is not required in the first instance.[18] Rather, social media materials must be relevant to the claims at issue.[19] "[T]he simple fact that a claimant has *had* social communications is not necessarily probative of the . . . issue in the case."[20]

In *McMillen v. Hummingbird Speedway, Inc.*, a Pennsylvania state court considered a defendant's motion to compel the plaintiff to produce log-in information for social media sites.[21] In response, the plaintiff asked the court to conclude that social media communications are essentially privileged; however, the court declined to do so, ordering the production of usernames and passwords to opposing counsel.[22] The court noted that while both Facebook and MySpace "do guarantee a modicum of privacy insofar as users may, with the exception of certain basic information, choose what information and posts to make public . . . reading their terms and privacy policies should dispel any notion that information one chooses to share, even if only with one friend, will not be disclosed to anyone else."[23]

The defendant in another Pennsylvania case, *Zimmerman v. Weis Markets, Inc.*, also sought user name and password information to access non-public portions of the plaintiff's social media profiles for information probative on damages issues.[24] The court there agreed with the *McMillen* rationale that no privilege protects social media postings under Pennsylvania law and accordingly granted the motion to compel.[25] The court "flatly rejected" the plaintiff's suggestion that the court should conduct an *in camera* review of the social media, as doing so would impose an unfair burden on the court.[26] Most recently, a third Pennsylvania court reiterated in *Largent v. Reed* that no general privacy or social media privilege

14. *Simply Storage Mgmt.*, 270 F.R.D. at 432.
15. *Id.* at 432–33.
16. *Id.* at 434.
17. *Id.*
18. *Id.* at 435.
19. *Id.*
20. *Id.*
21. No. 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *1 (Pa. D. & C. Sept. 9, 2010).
22. *Id.* at *3–4; *see also* Gallion v. Gallion, No. FA114116955S, 2011 Conn. Super. LEXIS 2517, at *1 (Super. Ct. Sept. 30, 2011) (ordering the exchange of parties' Facebook usernames and passwords between counsel only).
23. *McMillen*, 2010 Pa. Dist. & Cnty. Dec. LEXIS 2517, at *6.
24. Zimmerman v. Weis Mkts., Inc., No. CV-09-1535, 2011 Pa. Dist. & Cnty. Dec. LEXIS 187, at *6 (Pa. D. & C. May 19, 2011).
25. *Id.* at *3–4.
26. *Id.* at *3 n.2. *Compare* Offenback v. L.M. Bowman, Inc., No. 1:10-CV-1789, 2011 U.S. Dist. LEXIS 66432, at *7–10 (M.D. Pa. June 22, 2011) (citing *Simply Storage* for the scope of social media

protects Facebook profile information, even when designated as "private," including photographs, applications, posts, and status updates, from production.[27] The court wrote that "Facebook's foremost purpose is to 'help you connect and share with the people in your life.' That can only be accomplished by sharing information with others. Only the uninitiated or foolish could believe that Facebook is an online lockbox of secrets."[28]

In 2012, a Michigan federal court held similarly in *Tompkins v. Detroit Metropolitan Airport* that claims of privilege generally do not protect information posted on social media sites, although the court also recognized that the protections provided by Rule 26(b) apply to social media discovery.[29] In *Tompkins*, the plaintiff claimed that a back injury had impaired her ability to work and enjoy life.[30] Citing *McMillen*, the defendant moved to compel production of the plaintiff's entire Facebook account.[31] The court agreed with the holding of *McMillen* but stated that "the Defendant does not have a generalized right to rummage at will through information that Plaintiff has limited from public review. Rather, consistent with Rule 26(b) . . . there must be a threshold showing that the requested information is reasonably calculated to lead to the discovery of admissible evidence."[32] As the court warned, "[o]therwise, the Defendant would be allowed to engage in the proverbial fishing expedition in the hope that there *might* be something of relevance in Plaintiff's Facebook account."[33] The court denied the motion to compel, distinguishing the factual setting from *McMillen* and noting that none of the pictures the defendants attached as exhibits were inconsistent with the plaintiff's injury claims.[34]

The case law to date has not addressed one potential complication from orders directing parties to turn over social media passwords: contractual issues arising from the sites' terms of use.[35] Sites' terms of use, such as Facebook's Statement of Rights and Responsibilities, purport to preclude users from sharing their passwords with others.[36] A court order directing a Facebook user to provide sign-on

discovery and conducting an *in camera* review, using the plaintiff's username and password, to determine a limited list of materials that were discoverable from the plaintiff's Facebook account).

27. No. 2009-1823, slip op. at 9–10 (Pa. D. & C. Nov. 8, 2011).

28. *Id.* at 10; *see generally* Juror No. One v. Superior Ct., No. C067309, slip op. at 15–16 (Cal. Ct. App. May 31, 2012) (dismissing challenge to order directing juror to consent to disclosure of Facebook postings in connection with investigation of juror misconduct).

29. 278 F.R.D. 387, 388 (E.D. Mich. 2012).

30. *Id.* at 387.

31. *Id.* at 388.

32. *Id.*

33. *Id.*

34. *Id.* at 389.

35. The courts in both *Largent* and *McMillen* cite to Facebook's privacy policy in their privilege analysis but do not address the issue of compelling production of usernames and passwords. *See* Largent v. Reed, No. 2009-1823, slip op. at 9 (Pa. D. & C. Nov. 8, 2011); McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *6–9 (Pa. D. & C. Sept. 9, 2010).

36. *See, e.g.*, Facebook Statement of Rights and Responsibilities, FACEBOOK.COM, http://www.faceboook.com/legal/terms (last visited Feb. 14, 2012) ("Registration and Account Security . . . . 8. You will not share your password, . . . let anyone else access your account, or do anything else that might jeopardize the security of your account.").

information to an opposing party or counsel appears to compel the party to violate Facebook's terms of use. Although it is not clear at this point what consequences (if any) follow from the discrepancy between a court order and sites' terms of use, courts likely will have to confront that issue. By contrast, orders directing a user to turn over the contents of his or her social media postings do not seem to raise similar concerns.[37]

B. Discovery Requests to Social Media Providers

In contrast to courts' receptiveness to social media discovery directed to parties, litigants have been largely unsuccessful in seeking to compel entities that host social media sites to produce information data. In response to subpoenas requesting such data, those entities have relied on a 1986 federal statute, the Stored Communications Act (the "SCA"), as a shield against production.[38] The SCA prevents providers of communication services from disclosing private communications under specified circumstances. The statute restricts providers from voluntarily disclosing information in their possession about their users, and limits the government's ability to compel providers to divulge such information.[39]

A 2010 federal case from California, *Crispin v. Christian Audigier, Inc.*, provides a careful analysis of the SCA's provisions in the social media context.[40] *Crispin* arose out of a dispute concerning an oral license to use art in connection with the manufacture of certain apparel.[41] The defendants served subpoenas on Facebook, MySpace, and other third parties, seeking the plaintiff's communications and subscriber information.[42] The defendants contended that the information sought was relevant to the nature and terms of the alleged oral agreement.[43] The plaintiff filed an ex parte motion to quash the subpoenas, arguing, *inter alia*, that they sought information that the social media sites were prohibited from disclosing under the SCA.[44] The magistrate judge denied the motion to quash.[45]

37. *See Facebook Data Use Policy, Sharing and Finding You on Facebook*, Facebook.com, https://www.facebook.com/about/privacy/your-info-on-fb#controlprofile (last visited Feb. 14, 2012) (explaining that users' control over access to their information is not absolute and can be modified by other users to a certain extent); *Facebook Statement of Rights and Responsibilities*, Facebook.com, https://www.facebook.com/legal/terms?ref=pf (last visited Feb. 15, 2012) ("2. Sharing Your Content and Information. You own all of the content and information you post on Facebook . . . ."); *see also McMillen*, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, at *7 ("Facebook users are thus put on notice that regardless of their subjective intentions when sharing information, their communications could nonetheless be disseminated by the friends with whom they share it, or even by Facebook at its discretion.").

38. 18 U.S.C. §§ 2701–2712 (2006 & Supp. III 2009).

39. *Id.* §§ 2702–2703.

40. 717 F. Supp. 2d 965 (C.D. Cal. 2010).

41. *Id.* at 968.

42. *Id.*

43. *Id.* at 969.

44. *Id.*

45. *Id.*

The plaintiff moved for reconsideration before the district court on the issue of whether social media sites are subject to the SCA.[46] The district court granted that motion, and noted that the SCA prohibits communication service providers from disclosing private communications to specified entities.[47] The SCA "creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information."[48]

As an initial matter, the court determined that the plaintiff had standing to challenge the subpoenas due to the personal information at stake.[49] The court then turned to the SCA, noting that the statute distinguishes between providers of remote computing services ("RCS") and electronic communication services ("ECS").[50] The SCA defines RCS to be "the provision to the public of computer storage or processing services by means of an electronic communications system," while an ECS is defined to be "any services which provides to users thereof the ability to send or receive wire or electronic communications."[51] The SCA restricts disclosures by both RCS and ECS providers, under different legal tests.[52]

Recognizing that social media sites provide services beyond the contemplation of Congress in 1986, the court looked to legislative history as well as the application of the SCA to other technologies like text messages.[53] The court divided its analysis between messages that have been read and retained by a user on the social media site and those that have not been read.[54] The court concluded that the sites' unread private message services qualify the sites as ECS providers under the SCA.[55] The court also concluded that the social media sites qualify as RCS providers with respect to messages that have been opened and retained by a user.[56] The court decided that Facebook and MySpace are not ECS providers in connection with wall postings or comments; the court held that the social media sites were SCA-protected RCS providers with respect to such messages.[57] However, the record before the court did not indicate whether the plaintiff's

46. *Id.* at 971.

47. *Id.* at 970–71.

48. *Id.* at 972 (citing Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1213 (2004)).

49. *Id.* at 976.

50. *Id.* at 978–79 (citing 18 U.S.C. § 2511(2)).

51. *Id.* at 972 (citing 18 U.S.C. § 2510(15)).

52. *See* 18 U.S.C. § 2702 (2006). An ECS is prohibited from disclosing "the contents of a communication while in electronic storage by that service." *Id.* § 2702(a)(1). An RCS is prohibited from disclosing the content of any communication received by electronic transmission that is carried or maintained on its service for a customer "solely for the purpose of providing storage or computing processing services to [the] subscriber or customer, if the provider is not authorized to access the contents of [the] communications for the purpose of providing . . . services other than storage or computer processing." *Id.* § 2702 (a)(2).

53. *Crispin*, 717 F. Supp. 2d at 979.

54. *Id.* at 987.

55. *Id.* at 982.

56. *Id.* at 987.

57. *Id.* at 990. However, the court in *Juror No. One v. Superior Court* attempted to discount the conclusion of *Crispin*: "*Crispin* . . . did not establish as a matter of law that Facebook is either an ECS or an RCS or that the postings to that service are protected by the SCA. The findings in *Crispin*

privacy settings allowed the general public to view his wall postings and MySpace comments. As a result, the court reversed the magistrate judge's order with respect to private social media messages and remanded for further proceedings with respect to the plaintiff's Facebook wall postings and MySpace comments.[58]

C. Rule 34: The Cloud's Silver Lining

Although lawyers may find the idea of retrieving data from the cloud to be a fuzzy concept, cloud computing simply refers to storing data on a third party's infrastructure and using internet-based software to access that data.[59] For purposes of discovery, the principles resemble those controlling social media information: users typically will be found to have "possession, custody or control" of data that they upload to the cloud.[60]

In re NTL Inc. Securities Litigation, a 2007 decision in a securities action from the Southern District of New York, laid out the principles involved.[61] The defendant entity issued a document hold memorandum to a selected group of its employees.[62] Shortly after the plaintiffs brought suit, the defendant filed a Chapter 11 petition and its principal assets were divided between two new entities, only one of which became a defendant in the securities action.[63] The defendant successor entity did not produce any documents to the plaintiffs, on the ground that it did not have possession of the original defendant's documents because those materials were in the possession of the non-party successor.[64] The court disagreed, holding that the successor defendant had control for purposes of Rule 34(a).[65] "Under Rule 34, 'control' does not require that the party have legal ownership or actual physical possession of the documents at issue; rather, documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the document from a non-party to the action."[66] Because the defendant entity had a contractual right to access data owned by the non-party successor, the court found that the defendant successor had committed spoliation and imposed an adverse inference sanction.[67]

A 2009 decision from a federal court in Maryland illustrates the flip side of the control analysis.[68] In *Goodman v. Praxair Services, Inc.*, the plaintiff filed a

were based on the stipulations and evidence presented by the parties in that case." No. C067309, slip op. at 12 (Cal. Ct. App. May 31, 2012).

58. *Crispin*, 717 F. Supp. 2d at 991.

59. For a brief background on cloud computing, see, for example, Mark L. Austrian & W. Michael Ryan, *Cloud Computing Meets E-Discovery*, Cyberspace Law., July 2009, at 1.

60. *In re* NTL, Inc. Sec. Litig., 244 F.R.D. 179 (S.D.N.Y. 2007).

61. *Id.* at 181.

62. *Id.* at 182–83.

63. *Id.* at 181.

64. *Id.* at 184, 195.

65. *Id.* at 195.

66. *Id.* (internal citations omitted).

67. *Id.* at 201.

68. Goodman v. Praxair Servs., Inc., 632 F. Supp. 2d 494, 514 (D. Md. 2009).

spoliation motion that argued that the defendant had failed to preserve evidence when it knew or should have known of the potential for litigation.[69] One issue concerned whether the defendant was under a duty to preserve data in the possession of third-party consultants.[70] The plaintiff contended that the consultants were the defendants' agents, while the defendant argued that the consultants were independent contractors who were beyond its control.[71] Citing *NTL*, the court undertook a fact-intensive control analysis and concluded that the defendant did not have "sufficient legal authority or practical ability to ensure the preservation of documents prepared [by the third-party consultants]."[72] The court found that the plaintiff had failed to show the existence of a relationship comparable to the contractual file-sharing relationship found in *NTL*.[73] Accordingly, the court denied the portion of the motion relating to the third-party consultants.[74]

Future disputes over access to data stored in the cloud are likely to turn on the same kind of control analysis. If a party has the legal or practical ability to retrieve data stored on third-party computers, then a court likely will impose on the party the responsibility to preserve and produce that data.

III. New Developments in Old ESI

Even as developments in connection with social media and the cloud capture attention, the law governing more traditional forms of electronically stored information like e-mail continues to change with the technological times as well. We focus here on developments in connection with predictive coding and privacy issues.

A. Predictive Coding: Breaking the Code?

Both courts and commentators have bemoaned the expense involved reviewing the large volumes of data retained by modern computer systems.[75] We previously have noted that court-based projects like the Seventh Circuit Electronic Discovery Pilot Program are addressing that problem from a legal perspective, encouraging cost-reduction through approaches that include cooperation and

69. *Id.* at 505.
70. *Id.* at 512.
71. *Id.* at 514.
72. *Id.* at 515.
73. *Id.*
74. *Id.* at 525.
75. *See, e.g.*, Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 311 (S.D.N.Y. 2003) ("As individuals and corporations increasingly do business electronically—using computers to create and store documents, make deals, and exchange e-mails . . . the universe of discoverable material has expanded exponentially. The more information there is to discover, the more expensive it is to discover all the relevant information until, in the end, 'discovery is not just about uncovering the truth, but also about how much of the truth the parties can afford to disinter.'"); Steven C. Bennett, *Are E-Discovery Costs Recoverable by a Prevailing Party?*, 20 Alb. L.J. Sci. & Tech. 537, 538 n.1 (2010) (noting that a mid-size case can cost between $2.5 and $3.5 million for the collection, review, and production of electronic information).

respect for proportionality.[76] Technological approaches also are coming to the fore, including predictive coding—a software-based approach that uses sophisticated algorithms to locate relevant materials—in lieu of document-by-document review or a mechanical application of search terms.[77]

Case law addressing predictive coding is now beginning to appear. In *Da Silva Moore v. Publicis Groupe*,[78] Magistrate Judge Peck issued an opinion that "recognize[d] that computer-assisted review is an acceptable way to search for relevant ESI in appropriate cases."[79] As Judge Peck explained, "every person who uses email uses predictive coding, even if they do not realize it. The 'spam filter' is an example of predictive coding."[80] Unlike traditional document review, predictive coding involves attorneys coding a small set of documents, which the computer uses to code other documents, until the system's predictions and reviewers' coding are sufficiently aligned.[81]

Da Silva Moore was a gender discrimination case, in which five female plaintiffs asserted claims against a large advertising conglomerate.[82] As part of a phased discovery process, the parties agreed to employ predictive coding to create a random sample of e-mail data and to use that collection to train the predictive coding software.[83] The defendants agreed to provide the entire sample set, with coding, to the plaintiffs for their review prior to running the predictive coding on the remaining e-mail collection.[84]

After the parties submitted an ESI protocol to the court,[85] the plaintiffs objected to the protocol in three primary respects. First, the plaintiffs asserted that predictive coding "provides unlawful 'cover' " for defendants' counsel to escape their Rule 26(g) duty to certify that production is complete and correct.[86] Judge Peck rejected that contention, noting that in "large-data cases like this, involving over three million emails, no lawyer using any search method could honestly certify its production is 'complete'—but more importantly, Rule 26(g)(1)

76. *See* Timothy J. Chorvat & Laura E. Pelanek, *Electronically Stored Information in Litigation*, 67 BUS. LAW. 285, 291 (2011); Timothy J. Chorvat & Laura E. Pelanek, *Electronically Stored Information in Litigation*, 66 BUS. LAW. 183, 188–89 (2010). The Pilot Program recently completed its second phase and is now expanding to additional courts and cases in Phase Three. *See* SEVENTH CIRCUIT ELEC. DISCOVERY PILOT PROGRAM COMM., SEVENTH CIRCUIT ELECTRONIC DISCOVERY PILOT PROGRAM: FINAL REPORT ON PHASE TWO, MAY 2010–MAY 2012, at 1 (2012), *available at* http://www.discoverypilot.com/sites/default/files/Phase-Two-Final-Report-Appendix.pdf. The Pilot Program's website, www.discoverypilot.com, includes discussions of recent cases involving ESI as well as links to further web-based ESI resources.

77. Da Silva Moore v. Publicis Groupe, No. 11 Civ. 1279 (ALC) (AJP), 2012 U.S. Dist. LEXIS 23350, at *3 (S.D.N.Y. Feb. 24, 2012) (citing Andrew Peck, *Search, Forward*, L. TECH. NEWS, Oct. 2011, at 25, 29).

78. *Id.*

79. *Id.*

80. *Id.* at *7 n.2.

81. *Id.* at *6.

82. *Id.* at *4.

83. *Id.* at *14, *16.

84. *Id.* at *16.

85. *Id.* at *20 n.6.

86. *Id.* at *20.

does not require that."[87] Second, the plaintiffs objected that predictive coding violates the "gatekeeping function" of Federal Rule of Evidence 702.[88] However, Judge Peck concluded that Rule 702 does not apply because the e-mails located by predictive coding are "not being offered into evidence at trial as the result of a scientific process or otherwise. The admissibility of specific emails at trial will depend upon each email itself."[89] Third, the plaintiffs objected to the ESI protocol on the basis that it lacks a standard to determine whether the method is reliable.[90] Judge Peck described this objection as premature.[91]

Judge Peck observed that his opinion appeared to be the first to endorse the use of predictive coding, but specifically noted that it was not intended to mandate predictive coding.[92] Judge Peck specifically stated that predictive coding does not have to be used in all cases.[93] Similarly, the court recognized that the ESI protocol approved in *Da Silva Moore* may not be appropriate in other situations.[94] Judge Peck concluded that "[w]hat the Bar should take away from this Opinion is that computer-assisted review is an available tool and should be seriously considered for use in large-data-volume cases where it may save the producing party (or both parties) significant amounts of legal fees in document review."[95]

B. Privacy Concerns

In *Corsair Special Situations Fund, L.P. v Engineered Framing Systems, Inc.*,[96] a collection action, a defendant and judgment debtor filed a motion to quash a subpoena directed to Verizon Wireless that sought information relating to her account.[97] The defendant argued that the subpoena violated her right to privacy and would be duplicative of other disclosed information.[98] The defendant did not cite any authority supporting her privacy argument, but the court analyzed what it saw as analogous claims of a right to privacy in billing information.[99] The court concluded that no right to privacy protects the account information contained in invoices, such as dates of account and roaming fees.[100] Noting a circuit split on the right to a protected privacy interest in the contents of text messages, the court found that the defendant failed to carry her burden to show that she had standing to challenge the subpoena.[101] Accordingly, the court denied the

87. *Id.* at *21.
88. *Id.* at *23.
89. *Id.* at *24.
90. *Id.*
91. *Id.* at *25.
92. *Id.* at *39–40.
93. *Id.* at *40.
94. *Id.*
95. *Id.*
96. No. 09-1201-PWG, 2011 U.S. Dist. LEXIS 91770, at *3 (N.D. Md. Aug. 17, 2011).
97. *Id.*
98. *Id.*
99. *Id.* at *7–10.
100. *Id.* at *7–8.
101. *Id.* at *10.

motion to quash, although the court ordered that information produced in response to the subpoena could be used only for the limited purpose of collecting the judgment. Once the judgment was satisfied, all copies of the information were to be destroyed or returned within thirty days.[102]

IV. Conclusion

As in past years, recent developments in the law of electronically stored information are noteworthy—principally for the application of existing principles to new technologies, rather than for the creation of novel legal doctrines. The rule that a party must preserve and produce information within its possession, custody, or control will continue to provide the starting point for a determination of whether data are producible, without regard to what individual or entity owns the machine on which the data reside.

102. *Id.* at *11.

Survey of E-Contracting Cases: Browsewrap, Clickwrap, and Modified Clickwrap Agreements

*By Deborah Davis Boykin**

E-contracting is a method of creating contracts over the internet; E-contracting has not changed the principles of contract formation and interpretation.[1] The two most common types of electronic agreements are "clickwrap" and "browsewrap" agreements.[2] Clickwrap and browsewrap agreements are distinguishable by whether they require an affirmative action on the part of the user to manifest assent to their respective terms, such as clicking an "Accept" or "I agree" button. With clickwrap agreements (also referred to as "clickthrough"), the webpage user manifests assent to the terms of a contract by clicking an "accept" button in order to proceed.[3] By contrast, browsewrap agreements (also referred to as "browserwrap") do not require the webpage user to perform an affirmative act of assent; the user does not need to sign a document or click an "accept" or "I agree" button.[4] "Modified clickwrap" agreements are hybrid browsewrap and clickwrap arrangements in which the user must affirmatively assent to the terms of an agreement: "the customer is told that consequences will necessarily flow from his assenting click and also is placed on notice of how or where to obtain a full understanding of those consequences."[5] Browsewrap, clickwrap, and, more recently, "modified clickwrap" cases continue to test the enforceability

* Deborah Davis Boykin is an attorney and a software licensing specialist in northern California.

1. Van Tassell v. United Mktg. Grp., LLC, 795 F. Supp. 2d 770, 789 (N.D. Ill. 2011) ("The making of contracts over the internet 'has not fundamentally changed the principles of contract.' " (quoting Register.com v. Verio, Inc., 356 F.3d 393, 403 (2d Cir. 2004)); *id.* ("Thus, the basic tenet of contract law remains unchanged: in order to be binding, a contract requires a 'meeting of the minds' and a manifestation of 'mutual assent.' " (quoting Agritrack, Inc. v. DeJohn Housemoving, Inc., 25 P.3d 1187, 1192 (Colo. 2001)).

2. *Id.* at 790.

3. *Id.*

4. *See, e.g.*, *id.* ("Unlike with clickwrap agreements, browsewrap agreements do 'not require the user to manifest assent to the terms and conditions expressly—the user need not sign a document or click an "accept" or "I agree" button.' Instead, browsewrap agreements typically 'involve a situation where notice on a website conditions use of the site upon compliance with certain terms or conditions, which may be included on the same page as the notice or accessible via a hyperlink.' " (quoting Sw. Airlines v. BoardFirst, L.L.C., 06-CV-0891-B, 2007 WL 4823761, at *4 (N.D. Tex. Sept. 12, 2007)).

5. Vernon v. Qwest Commc'ns Int'l, Inc., No. 09-cv-01840-RBJ-CBS, 2012 WL 768125, at *11 (D. Colo. Mar. 8, 2012).

of terms and conditions that are posted on a website. This survey discusses such recent cases.

I. Browsewrap Cases

In *Van Tassell v. United Marketing Group, LLC*,[6] the U.S. District Court for the Northern District of Illinois decided whether the plaintiffs assented to an arbitration clause that was contained within a browsewrap on the defendants' websites. The defendants (United Marketing, Taylor Gifts, and Pikes Peak) filed a joint motion to compel arbitration based on the arbitration provision in the "Terms and Conditions" purportedly displayed on the various websites used by the plaintiffs.[7] Pikes Peak, relying on the rulings in *Hubbert v. Dell Corp*.[8] and *PDC Laboratories, Inc. v. Hach Co*.[9] that upheld the validity of their respective browsewrap agreements, argued "because Van Tassell used the website and made a purchase on the website, she agreed to be subject to the Conditions of Use found on the website, which mandate arbitration of all disputes."[10]

To decide whether the arbitration clause was enforceable, the court had to determine whether actual or constructive knowledge of the terms and conditions was present.[11] The court viewed Pike Peak's web pages on its website (ChefsCatalog.com) and hyperlinks to determine whether they provided reasonable notice of the terms and conditions and found the following:

> [T]he notice of the Conditions of Use on ChefsCatalog.com is far less conspicuous than the notice in the cases upon which Pikes Peak relies. Unlike in either *Hubbert* or *PDC Laboratories*, a hyperlink to the Conditions of Use does not appear on either the home page or the checkout pages. Instead, a user only encounters the Conditions of Use after scrolling to the bottom of the home page and clicking the "Customer Service" link, and then scrolling to the bottom of the Customer Service page or clicking the "Conditions of Use, Notices & Disclaimers" link located near the end of a list of links on the page.[12]

The court concluded "the absence of any reference to the Conditions of Use coupled with the multi-step process to locate the Conditions of Use" means that . . . users of the ChefsCatalog.com website could complete their purchases without ever having notice that their purchases are subject to the website's Conditions of Use."[13] The court held that the defendants' multi-step processes failed

6. *Van Tassell*, 795 F. Supp. 2d at 790.
7. *Id*. at 787.
8. 835 N.E.2d 113 (Ill. App. Ct. 2005).
9. PDC Labs., Inc. v. Hach Co., No. 09-1110, 2009 WL 2605270 (C.D. Ill. 2009).
10. *Van Tassell*, 795 F. Supp. at 792.
11. *Id*. at 791 ("Thus, absent a showing of actual knowledge of the terms by the webpage user, the validity of a browsewrap contract hinges on whether the website provided reasonable notice of the terms of the contract.").
12. *Id*. at 792.
13. *Id*. at 793.

to provide the plaintiffs reasonable notice of the Conditions of Use and denied the defendants' motion to compel arbitration.[14]

In March 2012, a New York district court reached a similar conclusion where the defendants' browsewrap was inconspicuously placed on the defendants' website.[15] In *Jerez v. JD Closeouts, LLC*, a New York buyer filed a claim in his home state against a Florida seller.[16] The seller responded with a motion to dismiss based on a forum selection clause contained within the Terms of Sale ("Terms").[17] The motion was supported by an affidavit in which the principal owner asserted that all sales transacted on the company's website were conditioned by the Terms found by following a hyperlink, which was located on its "About Us" web page.[18] The facts revealed that the Terms were difficult to find, the buyer never saw them, and "[the Terms] were 'buried' and 'submerged' on a webpage that could only be found by clicking on an inconspicuous link on the company's 'About Us' page."[19] Citing *Fteja v. Facebook, Inc*.[20] and *Hoffman v. Supplements Togo Management, LLC*,[21] the court found the defendants' Terms "were submerged too deeply to become a binding part of any sale agreement" and denied their motion to dismiss.[22] The court provided the following standard for a seller in an e-commerce transaction:

> [A] seller must make an affirmative effort to "reasonably communicate" the essential terms of sale to the buyer. If it wishes to make those terms part of the bargain, it can easily do so by providing notice to the buyer that the terms can be found at a given website address . . . [or by structuring] their website in a manner that placed the terms of sale directly up front, in a conspicuous place, for all to see.[23]

II. Modified Clickwrap Cases

In August 2011, the U.S. District Court for the District of Northern California addressed a similar issue in *Swift v. Zynga Game Network, Inc*.[24] regarding whether the plaintiff assented to an arbitration provision contained in a modified clickwrap. Swift argued that Zynga's modified clickwrap provided insufficient

14. *Id.*
15. Jerez v. JD Closeouts, LLC, 943 N.Y.S.2d 392 (Dist. Ct. Nassau Cnty. 2012).
16. *Id.* at 393.
17. *Id.*
18. *Id.* at 394–95.
19. *Id.* at 398.
20. No. 11 Civ. 918 (RJH), 2012 WL 183896, at *5 (S.D.N.Y. Jan. 24, 2012) (enforcing a forum selection provision where the sign-up page provided: "By clicking Sign Up, you are indicating that you have read and agree to the Terms of Service," and the phrase "Terms of Service" was a hyperlink to such Terms of Service).
21. 18 A.3d 210, 219–20 (N.J. Super. Ct. App. Div. 2011) (ruling that the forum selection provision was presumptively unenforceable because it "was unreasonably masked from the view of the prospective purchasers because of its circuitous mode of presentation"), *cert. granted*, 36 A.3d 1063 (N.J. 2012).
22. *Jerez*, 943 N.Y.S.2d at 398–99.
23. *Id.* at 398.
24. 805 F. Supp. 2d 904 (N.D. Cal. 2011).

notice of the terms of service. The plaintiff, relying on the decision in *Specht v. Netscape Communications Corp.*,[25] argued that:

> "[M]ost internet and software transactions use a "clickwrap" process to obtain a user's consent to terms of service whereby the terms of service are presented on the screen and do not allow the user to proceed without clicking to assent to the terms. Plaintiff contrasts this process with the procedure for consenting to YoVille's TOS, where the terms of service are not visible on the page but instead are linked by the blue hyperlink within a smaller grey font following the "Allow" button, which also relates to allowing access to Facebook information. Plaintiff contends that this "modified clickwrap" was insufficient to put her on notice of what she was assenting to, so she is not bound by the YoVille TOS or the Universal TOS.[26]

However, the court contrasted the facts in *Specht*[27] with the facts of the present case, in which "[Swift] admits that she was required to and did click on an 'Accept' button directly above a statement and that clicking on the button served as assent to the YoVille terms of service along with a blue hyperlink directly to the terms of service."[28] On these facts, the court found that the plaintiff was provided with an opportunity to review the terms of service and held that a binding contract was created.[29]

In March 2012, the U.S. District Court for the Northern District of Illinois was faced with another arbitration issue in *Sherman v. AT&T Inc.*[30]: whether to grant AT&T's motion to compel arbitration in accordance with the provisions of its terms of service. The facts showed that:

> To activate his internet service, [Sherman] was required to complete an online registration process, during which he was asked to check a box labeled "I have read and agree to the AT&T Terms of Service, Acceptable Use Policy, AT&T and Yahoo Privacy Policies, [and] Wi-Fi Terms of Service." On that same screen, "AT&T Terms of Service" linked to the AT&T Terms of Service.[31]

Shortly thereafter, AT&T revised its Terms and provided notice thereof "to its customers by sending them an email containing information about the revision, a link to the full text of the Terms and a reminder that '[b]y continuing to use the Service, you are agreeing' to the Terms."[32] Based on the decisions cited in prior clickwrap cases[33] and the finding that "Sherman does not deny and cannot deny

25. 306 F.3d 17 (2d Cir. 2002).
26. *Swift*, 805 F. Supp. 2d at 910.
27. *Specht*, 306 F.3d at 32 ("[W]here consumers are urged to download free software at the immediate click of a button, a reference to the existence of license terms on a submerged screen is not sufficient to place consumers on inquiry or constructive notice of those terms.").
28. *Swift*, 805 F. Supp. 2d at 911.
29. *Id.* at 912.
30. No. 11 C 5857, 2012 WL 1021823 (N.D. Ill. Mar. 26, 2012).
31. *Id.* at *1 (internal citation omitted).
32. *Id.* (alteration in original).
33. *See*, *e.g.*, Treiber & Straub Inc. v. United Parcel Serv., Inc., 474 F.3d 379, 385 (7th Cir. 2007) (finding a clickwrap process "provided adequate notice" to customers when the consumer was required to click to manifest assent and the terms both repeated the disclaimer of liability several times and referred to the contract available on the business's website).

that he actively clicked that he accepted the hyperlinked Terms," the court held that "Sherman had adequate notice of the Terms, to which he assented at the time of his activation of internet service" and granted AT&T's motion to compel arbitration.[34]

In March 2012, the U.S. District Court for the District of Colorado further described browsewrap, clickwrap, and hybrid arrangements in *Vernon v. Qwest Communications International, Inc*.[35] The court described a hybrid arrangement (or "modified clickwrap") as follows:

> [T]he customer must take affirmative action—pressing a "click" button—but, like a browsewrap agreement, the terms being accepted do not appear on the same screen as the accept button, but are available with the use of [a] hyperlink. Under this hybrid arrangement, the customer is told that consequences will necessarily flow from his assenting click and also is placed on notice of how or where to obtain a full understanding of those consequences.[36]

The court found that regardless of the scenario (browse, click, or hybrid), the threshold issues are the same: "[1] did the consumer have reasonable notice, either actual or constructive, of the terms of the putative agreement and [2] did the consumer manifest assent."[37]

Thus, the court's first substantive determination was whether the plaintiffs entered into the Subscriber Agreement and had sufficient notice of the arbitration clause therein. The facts showed that, in December 2005, Qwest provided its customers notice of its new Subscriber Agreement in a letter that stated in bold: " 'Qwest will assume you have accepted these terms unless you contact Qwest within 30 days of your transfer date.' "[38] Qwest also informed its customers that " 'more information on Qwest High-Speed Internet service terms and conditions' could be found 'at www.qwest.com/legal.' "[39] In addition, customers who enrolled in the new "Price for Life" program via the internet were required to check a box indicating that they agreed to the "Terms and Conditions" during the enrollment process, and Qwest further informed consumers of the location of the terms, and requested that consumers review the terms, on the checkout page.[40] Customers who signed up for an internet package over the telephone were also presented with notice of the Subscriber Agreement via a voice prompt system.[41] Although the plaintiffs maintained that they were not presented with the Subscriber Agreement, arguing that "proper 'presentation' or 'delivery' of the Subscriber Agreement and arbitration clause required that these provisions 'appear on the same scroll down or page as the "I Accept" and the "I Do Not Accept" buttons' during the installation process," the court found that Qwest provided

34. *Sherman*, 2012 WL 1021823, at *3, *5.
35. 09-cv-01840-RBJ-CBS, 2012 WL 768125 (D. Colo. Mar. 8, 2012).
36. *Id.* at *11.
37. *Id.*
38. *Id.* at *5.
39. *Id.*
40. *Id.* at *7.
41. *Id.*

the plaintiffs with sufficient notice of the Subscriber Agreement and the arbitration clause therein.[42]

Next the court decided whether the plaintiffs assented to the arbitration clause. The facts showed that "each of the Plaintiffs continued to use the high speed internet service for several months after installing the necessary software and receiving a Welcome Letter," both of which referenced the Subscriber Agreement.[43] Applying the state law for contract formation and citing relevant cases on this issue,[44] the court found that the plaintiffs voluntarily accepted the Subscriber Agreement and the arbitration provision.[45]

III. Conclusion

These recent cases show that courts are more willing to enforce the terms of a browsewrap and hybrid/modified clickwrap arrangement when the website user is provided adequate notice of the terms, evidenced by the reasonable placement of such terms on the website, and an adequate time to object to such terms. In addition, courts consistently enforce clickwraps where the website user checks an "Accept" or "I agree" box, and the clickwrap terms to which the user is assenting are reasonably available.

42. *Id.* at *12–13.

43. *Id.* at *14.

44. *See*, *e.g.*, Pierce v. St. Vrain Valley Sch. Dist. RE-1J, 981 P.2d 600, 603 (Colo. 1999) ("[T]he formation of a contract requires a bargain in which there is a manifestation of mutual assent to the exchange and a consideration." (alteration in original)); Mumm v. Adam, 307 P.2d 797, 801 (Colo. 1957) ("True assent may be implied from the circumstances and acts of the parties, but it must appear in some form."); Indus. Prods. Int'l, Inc. v. Emo Trans, Inc., 962 P.2d 983, 988 (Colo. App. 1997) ("A party may demonstrate assent to the terms of the offer . . . by promising to perform or by performing."); Loden v. Drake, 881 P.2d 467, 469 (Colo. App. 1994) ("[O]ne generally cannot avoid contractual obligations by claiming that he or she did not read the agreement.").

45. *Vernon*, 2012 WL 769125, at *14.

The Ethics of Lawyers Marketing Their Services on Daily Deal Websites

*By R. Michelle Boldon**

Recently, the state bars of Indiana, New York, South Carolina, and North Carolina issued ethics opinions on whether a lawyer may market legal services on "daily deal" and "group coupon" websites.[1] A daily deal is a marketing and sales tactic whereby a merchant offers a discount for a product or service via a daily deal website.[2] Examples of daily deals include discounts on products and services such as spa packages and restaurants.[3] The daily deal websites are intermediaries between merchants and consumers.[4] The Legal Ethics Committee of the Indiana State Bar Association ("Indiana Committee") concluded that the use of such websites by lawyers is a violation of its rules of professional conduct while the other states' committees found such marketing permissible if done within certain guidelines. This survey provides an overview of the two leading daily deal sites (Groupon.com and LivingSocial.com), the applicable ABA Model Rules of Professional Conduct ("Rules"),[5] and a brief analysis of the ethics opinions from Indiana, New York, South Carolina, and North Carolina.

How Do Groupon and LivingSocial Work?

Groupon is the largest daily deal website company and serves over 1,000 markets globally.[6] One of the key and distinguishing features of Groupon's business

* R. Michelle Boldon is an information technology (IT) professional turned attorney with over ten years of experience in the IT industry. She is a solo practitioner based in Houston, Texas concentrating in business and technology law.

1. *Opinion No. 1 of 2012*, Res Gestae, Apr. 2012, at 20 [hereinafter Ind. Ethics Op.]; N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 897 (2011), 2011 WL 7784110 [hereinafter N.Y. Ethics Op.]; S.C. Bar Ethics Advisory Comm., Op. 11-05 (2011), 2011 WL 7657361 [hereinafter S.C. Ethics Op.]; Council of N.C. State Bar, Formal Ethics Op. 10 (2011), *in* The North Carolina State Bar 2012 Lawyer's Handbook 10-226 (2012) [hereinafter N.C. Ethics Op.], *available at* http://www.ncbar.com/handbook/2012%20Handbook.pdf.

2. Erik Eliason, Yohanes Frezgi & Fatima Khan, Daily Deals White Paper: Understanding the Industry Dynamics of Daily Deals and Implications for Merchants and Consumers 3 (2010) [hereinafter Understanding the Industry], *available at* http://www.slideshare.net/HackStartups/groupbuying-white-paper.

3. *See, e.g.*, LivingSocial, http://www.livingsocial.com (last visited Aug. 2, 2012).

4. Understanding the Industry, *supra* note 2, at 4.

5. Model Rules of Prof'l Conduct (2009). All states have adopted the ABA Model Rules of Professional Conduct so those rules are cited throughout this survey, except in the section regarding Indiana.

6. Understanding the Industry, *supra* note 2, at 4.

model is that a deal is activated only if a certain "tipping point" is reached, that is, a certain number of consumers must purchase the voucher before the discount takes effect.[7] If that predetermined threshold is not reached, no one who signed up for the discount gets the deal.[8] Groupon collaborates with merchants to define the tipping point and determine what the discount should be, which will be somewhere between 45 percent and 90 percent of the original sales price.[9] Groupon and the merchant also agree to a fee-splitting arrangement, typically a fifty-fifty split of the revenue generated.[10] Once a deal is sold, Groupon collects the payments from customers and keeps a portion of the revenue from each Groupon sold.[11] The second leading daily deal website is LivingSocial.[12] LivingSocial also offers daily deals on products and services; LivingSocial's business model is similar to Groupon's except it does not require that a certain number of users purchase the deal for it to be activated.[13]

Applicable ABA Model Rules of Professional Conduct

In the ethics opinions discussed in this survey, the state bars examined the ethics of lawyers participating in the daily deal sales arrangements based on the Rules related to excessive fees, the safe-keeping of property, fee-sharing, advertising, and establishing the client-lawyer relationship.

Rule 1.5 provides that "[a] lawyer shall not make an agreement for, charge, or collect an unreasonable fee or an unreasonable amount for expenses."[14] Because a daily deal website user pays for the lawyer's service in advance, a lawyer might violate this rule if the lawyer were required to terminate representation or if the user never sought the discounted service.

Under Rule 1.15, a lawyer must deposit fees paid in advance into a client trust account, to be withdrawn as the fees are earned.[15] Additionally, Rule 1.16(d) states that a lawyer must return any advance payment or fee upon termination of representation.[16] According to LivingSocial's terms and conditions, the promotional part of a voucher will expire on the date printed on the voucher and the paid portion could expire five years from the date it was purchased, depending on the state.[17] The requirements of Rules 1.15 and 1.16 present challenges for lawyers who market their services using daily deal websites. For instance,

7. *Id.*
8. *Id.* Relatedly, when that threshold is not met, no one actually purchases the voucher. *Id.*
9. *Id.* at 15.
10. *Id.*
11. *Groupon FAQs*, GrouponWorks, http://www.grouponworks.com/merchant-services/FAQs (last visited Aug. 2, 2012).
12. Understanding the Industry, *supra* note 2, at 20.
13. *See* LivingSocial, http://www.livingsocial.com/ (last visited Aug. 2, 2012).
14. Model Rules of Prof'l Conduct R. 1.5(a) (2009).
15. *See id.* R. 1.15(c).
16. *See id.* R. 1.16(d).
17. *See, e.g.*, *Terms and Conditions*, LivingSocial, http://www.livingsocial.com/terms#expiration_dates (last modified July 17, 2012).

lawyers must take steps to stay within the bounds of professional conduct if a voucher expires or the daily deal user never seeks the lawyer's services.

The state bars also addressed the issue of impermissible fee-sharing because the websites pay a portion of the revenue to the lawyer. Rule 5.4 clearly states that "[a] lawyer or law firm shall not share legal fees with a nonlawyer."[18] In general, if the payment is deemed a payment for advertising and the advertising cost is reasonable, then there is no violation of the Rules; if the payment is deemed as part of a fee-splitting arrangement, then there may be a violation.[19] The ethics opinions varied as to how they defined advertising costs. Lawyers must ensure that the daily deal complies with Rules 7.1 and 7.2 on advertising.

The ethics committees also examined how a client-lawyer relationship is established. Users who take advantage of a daily deal are anonymous to the merchant. Is a client-lawyer relationship established once a user purchases a daily deal? The Rules do not specify what starts the relationship but all of the ethics committees agreed that coupon purchasers must be treated as prospective clients.[20]

Indiana's Ethics Opinion

The Indiana Committee addressed the question: "Can a lawyer licensed in Indiana use group coupon or daily deal marketing in compliance with Indiana's Rules of Professional Conduct?"[21] The Indiana Committee found that advertising through daily deal sites like Groupon "is likely not appropriate for a lawyer licensed in Indiana."[22]

The Indiana Committee found it troubling that, on a daily deal website, a prospective client may purchase the lawyer's services without the lawyer and client having a consultation.[23] Rule 2.1 of the Indiana Rules of Professional Conduct (the "Indiana Rules") states that "in representing a client, a lawyer shall exercise independent professional judgment and render candid advice."[24] According to the Indiana Committee, this standard is difficult to attain in the daily deal context where the anonymous potential client chooses the lawyer rather than the lawyer choosing to represent the client.[25]

The Indiana Committee reasoned that the arrangement of the daily deal website as the intermediary between a client and lawyer may be a violation of Indiana Rules Guideline 9.3: "a lawyer may not delegate to a non-lawyer assistant: (a) responsibility for establishing an attorney-client relationship."[26] The Indiana

18. Model Rules of Prof'l Conduct R. 5.4 (2009).
19. *See* Ind. Ethics Op., *supra* note 1, at 24; N.Y. Ethics Op., *supra* note 1, at *2 & n.3; S.C. Ethics Op., *supra* note 1, at *1; N.C. Ethics Op., *supra* note 1, at 10-226.
20. *See* Ind. Ethics Op., *supra* note 1, at 24–25; N.Y. Ethics Op., *supra* note 1, at *3; S.C. Ethics Op., *supra* note 1, at *1; N.C. Ethics Op., *supra* note 1, at 10-226.
21. Ind. Ethics Op., *supra* note 1, at 20, 22.
22. *Id.* at 25.
23. *Id.* at 20.
24. *Id.* (quoting Ind. Rules of Prof'l Conduct R. 2.1).
25. *Id.* at 20, 22.
26. *Id.* at 22 (quoting Ind. Rules of Prof'l Conduct Guideline 9.3).

Committee's perspective is that the attorney-client relationship is established as a result of the arrangement by the intermediary marketer rather than by the lawyer directly, which may be a violation of Guideline 9.3.[27]

The Indiana Committee stated that the daily deal sales arrangement creates an issue for the rule on the safekeeping of property, particularly Rule 1.15(c), which requires a lawyer to deposit legal fees that have been paid in advance into a client trust account.[28] Additionally, under Rule 1.15(a), a lawyer must keep "complete records" of a client's funds and keep those funds separated.[29] The opinion explains some of the variations of how the daily deal websites submit payment to the lawyer: (1) the merchant holds fees at the merchant's discretion and then disburses a part of the fees to the lawyer, (2) the merchant disburses fees to the lawyer in incremental amounts at a time, or (3) the lawyer agrees that funds deposited to the lawyer remain the property of the merchant.[30] From the Indiana Committee's perspective, online coupon advertising may be permissible in rare circumstances but it is difficult to see how the lawyer could comply with the requirements of Rule 1.15 given the variations of how the website companies submit payment to the lawyer.[31]

Furthermore, the Indiana Committee questioned how a lawyer can ethically decline or terminate a client's representation under Rule 1.16 which requires the lawyer to refund promptly to the client the entire amount of the fee paid.[32] The implication is that the lawyer may be prohibited from promptly making a full refund to the potential client because the website company could still have a portion of the client's fee when the lawyer determines that she cannot represent the client.[33] The Indiana Committee gives the example of a prospective client who purchases a daily deal for the lawyer to draft a durable healthcare power of attorney.[34] When the lawyer meets with the prospective client and discovers that the prospective client already has a durable healthcare power of attorney, the lawyer may not be able to refund 100 percent of the funds the prospective client paid because the daily deal company has a portion of the prospective client's fee and to withdraw funds for the refund from the lawyer's trust account (which contains other clients' funds) would be a violation of the Rules.[35]

Finally, according to the Indiana Committee, the use of daily deals sites is a violation of Indiana's fee-splitting and advertising rules.[36] According to the Indiana Committee, the use of the daily deals sites is a method of "channeling pro-

27. *Id.*
28. *Id.* at 22–23.
29. *Id.* at 22 (quoting Ind. Rules of Prof'l Conduct R. 1.15(a)).
30. *Id.* at 22–23.
31. *Id.* at 22.
32. *Id.* at 22–23.
33. *Id.* at 23.
34. *Id.* at 25 n.6.
35. *Id.*
36. *Id.* at 23–24.

fessional work," which is a violation of Rule 7.2.[37] Though Rule 7.2(b)(1) permits a lawyer to pay reasonable costs for advertising, a daily deal website company may keep up to fifty percent of the amount charged to the customer, a rate that the Indiana Committee does not deem reasonable.[38]

New York, South Carolina, and North Carolina Ethics Opinions

The New York, South Carolina, and North Carolina ethics committees (collectively, the "Committees") answered in the affirmative when they addressed the question of whether an attorney may market legal services on a daily deal website. The opinion of the Committee on Professional Ethics of the New York State Bar Association (the "New York Committee") added that not all legal services are suited to be marketed within the daily deals framework but the business model may be suitable for some services, like the drafting of a simple will.[39]

Establishing the Attorney-Client Relationship

Like the Indiana Committee, the New York Committee raised the issue of how the attorney-client relationship may be prematurely or improperly formed.[40] The New York Committee noted that "[t]he danger is that the arrangement could be taken to establish a lawyer-client relationship before the lawyer has had any opportunity to check for conflicts, determine whether the described legal services are appropriate for the consumer, and whether the lawyer is competent to provide those services."[41] The New York Committee instructed that these dangers could be avoided if the "deal of the day" were accompanied by the proper disclosures, including that the lawyer will conduct a conflicts check, the lawyer will determine if he is competent to provide the representation, and if the lawyer must decline representation he will give the prospective client a full refund.[42]

Advertising

As regards to advertising, as long as the lawyer pays a reasonable amount for advertising, the Committees agreed that advertising is allowed on the websites.[43] Additionally, the advertising must not be misleading or illusory.[44] The Council

37. *Id.* at 23 (quoting Ind. Rules of Prof'l Conduct R. 7.2 cmt. 4).
38. *Id.* at 24.
39. N.Y. Ethics Op., *supra* note 1, at *1.
40. *Id.* at *2.
41. *Id.* at *3.
42. *Id.* at *2.
43. *See* N.Y. Ethics Op., *supra* note 1, at *3; S.C. Ethics Op., *supra* note 1, at *1; N.C. Ethics Op., *supra* note 1, at 10-226; *see also* Ind. Ethics Op., *supra* note 1, at 22.
44. Model Rules of Prof'l Conduct R. 7.1 (2009).

of the North Carolina State Bar ("North Carolina Committee") identified specific concerns that must be addressed in the advertisement:

> The advertisement must explain that the decision to hire a lawyer is an important one that should be considered carefully and made only after investigation into the lawyer's credentials. In addition, the advertisement must state that a conflict of interest or a determination by the lawyer that the legal service being offered is not appropriate for a particular purchaser may prevent the lawyer from providing the service and, if so, the purchaser's money will be refunded . . . .[45]

It is noteworthy that only the Indiana Committee reported the cost of advertising with daily deal companies, which is typically 50 percent of the revenue collected from the coupon buyer. The New York Committee wrote that it was not aware of the amount daily deal website companies charge for advertising, and neither the Ethics Advisory Committee of the South Carolina Bar ("South Carolina Committee") nor the North Carolina Committee reported a cost.[46]

Advertising Fees vs. Fee Sharing

The Committees either concluded or inferred that the fees retained by a daily deal website company may be categorized as the cost of advertising on the daily deal website. The New York Committee reasoned that such fees are the cost of advertising and not fee-sharing because the websites do not have individual contact with the coupon buyers and the websites do not refer any particular lawyer.[47] It is also worth noting that the New York Committee stated it was not aware of the amount the websites charge for such advertising.[48] The New York Committee's conclusion is based on the assumption that the percentage of the amount retained is a reasonable payment.[49]

The South Carolina Committee categorized the fee retained by daily deal website companies as an advertising cost because the daily deal website deducts the fee for using the website upfront (as opposed to invoicing the lawyer and the lawyer paying for the service from her operating account).[50] The North Carolina Committee categorized the fee retained by the website company as the cost of advertising for a reason different from those stated by the New York and South Carolina Committees: because the amount is retained by the website company whether or not the coupon buyer claims the discounted service.[51]

The New York Committee also raised the issue as to whether the fees kept by the daily deal websites are improper payments for referrals and thus a violation of Rule 7.2(a), or allowable advertising fees.[52] The New York Committee an-

45. N.C. Ethics Op., *supra* note 1, at 10-226.
46. *See* N.Y. Ethics Op., *supra* note 1, at *2; S.C. Ethics Op., *supra* note 1, at *1–2; N.C. Ethics Op., *supra* note 1, at 10-226.
47. N.Y. Ethics Op., *supra* note 1, at *2.
48. *Id.* at *4 n.3.
49. *Id.* at *2.
50. S.C. Ethics Op., *supra* note 1, at *1.
51. N.C. Ethics Op., *supra* note 1, at 10-226.
52. N.Y. Ethics Op., *supra* note 1, at *2.

swered this question in the negative because it considered the websites to be an allowable mechanism to carry a lawyer's advertising message.[53]

The North Carolina Committee said that a daily deal sales arrangement is also a fee-splitting arrangement but falls within the fee-sharing limitations of the Rules because the website company (or nonlawyer) neither interacts with the lawyer nor interferes with the lawyer's independent judgment.[54] Rule 5.4(a) prohibits, with a few exceptions, a lawyer from sharing legal fees with a nonlawyer.[55] The South Carolina Committee also categorized the payment as a fee-splitting arrangement that does not violate Rule 5.4(a) "provided the website does not have the ability to exercise any control over the services which are to be subsequently rendered by the attorney."[56]

Excessive Fees

The New York Committee also raised the concern as to whether the amount received by a lawyer could result in an excessive fee violating Rule 1.5.[57] For instance, in some situations prospective clients may not receive the services to which they are entitled, the coupon buyer may want to discharge the lawyer, or perhaps the coupon buyer never seeks the lawyer's services.[58] The New York Committee instructs the bar that advance payments must be treated like retainers and, if an attorney is discharged without cause, the lawyer must give the client a full refund less any *quantum meruit* claim for services rendered.[59]

North Carolina requires its lawyers to deposit, in a trust account, any funds advanced by the website company.[60] If the purchaser does not claim the discounted service before the voucher expires, the lawyer must give the purchaser a full refund, or if the purchaser still desires the service, the lawyer may charge her actual rate and give the client credit for the advance payment.[61] The North Carolina Committee also stated that the lawyer may not charge the client an additional fee for the time the lawyer works beyond what she anticipated.[62] The lawyer must give the prospective client a full refund, including the funds retained by the website company, if the lawyer determines that the prospective client does not need the representation or that a conflict of interest exists.[63] The North Carolina Committee added in an end note: "In light of the many uncertainties of a legal representation arranged in the manner proposed, a lawyer may not condition the offer of discounted services upon the purchaser's

53. *Id.*
54. N.C. Ethics Op., *supra* note 1, at 10-226.
55. Model Rules of Prof'l Conduct R. 5.4(a) (2009).
56. S.C. Ethics Op., *supra* note 1, at *1.
57. N.Y. Ethics Op., *supra* note 1, at *2.
58. *Id.* at *3.
59. *Id.*
60. N.C. Ethics Op., *supra* note 1, at 10-226.
61. *Id.*
62. *Id.*
63. *Id.*

agreement that the money paid will be a flat fee or a minimum fee that is earned by the lawyer upon payment."[64]

Conclusion

The daily deal space is expected to continue to expand and develop.[65] Because of this trend, more state bar ethics committees may have to address the question as to whether advertising on daily deal websites is a violation of the Rules. Practitioners should consult their bar associations before launching ad campaigns on daily deal websites. As evidenced by the ethics opinions discussed in this survey, bar associations may vary in their analysis of daily deal websites and the Rules. For example, New York and the Carolinas each provided different reasons as to why the payment made by the website company to the lawyer is an advertising fee. If advertising is permitted, lawyers should proceed carefully and treat coupon buyers as prospective clients, deposit advance payments into their trust accounts, provide the necessary disclosures as required by adverting rules, and give the appropriate refund if a client fails to seek the discounted service or discharges the lawyer or the lawyer must terminate representation.

64. *Id.* at 10-226 n.1.
65. Understanding the Industry, *supra* note 2, at 12.

The European Union Model Interoperability Agreement for Electronic Business Documents

*By Phillip Schmandt**

Introduction

On February 15, 2012, the European Committee for Standardization (commonly referred to by its French acronym "CEN")[1] approved the Model Interoperability Agreement for Transmission and Processing of Electronic Invoices and Other Business Documents ("Model Interoperability Agreement").[2]

The Model Interoperability Agreement compliments the Model Trading Partner Agreement approved by both the European Commission and the American Bar Association in 1995.[3] However, while the Model Trading Partner Agreement was focused on electronic data interchange ("EDI"), the new Model Interoperability Agreement anticipates the exchange of documents that are written in Extensible Markup Language ("XML"). XML is a computer language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.[4] When prepared with XML, the exchanged documents can be automatically read by each of the trading parties' computer systems and integrated into their financial and other systems, thereby introducing significant efficiencies.[5]

* Phillip Schmandt is a partner in the law firm of McGinnis, Lochridge & Kilgore L.L.P. in Austin, Texas, where he is chair of the Technology Practice Group. Mr. Schmandt served as a Technical Expert to the European Union's standards body, the European Committee for Standardization (known as CEN, Comité Europeen de Normalisation), where he was responsible for drafting and editing the Code of Practice for Electronic Invoicing in the European Union. He was also a contributing author to the Model Interoperability Agreement that was approved by CEN on February 15, 2012.

1. Comité Europeen de Normalisation.

2. Eur. Comm. for Standardization, Model Interoperability Agreement for Transmission and Processing of Electronic Invoices and Other Business Documents (May 2012) [hereinafter Model Interoperability Agreement], *available at* ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA16464-2.pdf.

3. *See* Elec. Messaging Servs. Task Force, *The Commercial Use of Electronic Data Interchange: A Report and Model Trading Agreement*, 45 Bus. Law. 1645 (1990); Commission Recommendation (EC) No. 820/1994 of 19 Oct. 1994, Relating to the Legal Aspects of Electronic Data Interchange, 1994 O.J. (L 338) 98, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1994:338:0098:0117:EN:PDF.

4. Adrian Stevenson, *How to Find a Needle in a Haystack*, Institutional Web Mgmt. Workshop, at 21 (July 6, 2005), http://www.slideshare.net/adrianstevenson/how-to-find-a-needle-in-the-haystack.

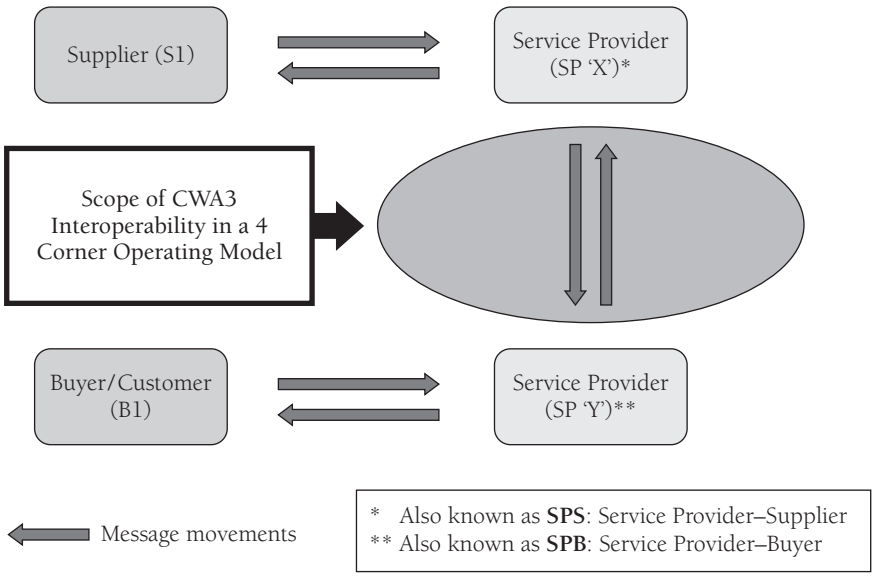
5. *European Commission Wants Broad Scale Adoption of e-Invoicing by 2020*, E-Invoicing Platform, at 1 (Dec. 2, 2010), http://eeiplatform.com/3374/european-commission-wants-broad-scale-adoption-of-e-invoicing-by-2020/.

The Model Interoperability Agreement is intended to facilitate the exchange of all electronic documents in the procurement to pay cycle, including purchase orders, change orders, invoices, and invoice acknowledgements.[6] Because of unique requirements in the European Union regarding the use of electronic invoices, the Model Interoperability Agreement pays particular attention to invoices, but anticipates that it will govern the exchange of all electronic business documents desired to be exchanged by the trading partners.[7]

What Is Interoperability?

The authors of the Model Interoperability Agreement recognized that the term "interoperability" is susceptible to many meanings.[8] In a companion document published simultaneously to explain the Model Interoperability Agreement, CEN reviewed a variety of definitions of "interoperability" that had been used in the past, but noted that for purposes of the Model Interoperability Agreement the term interoperability was intended to mean only the following:

> While recognizing there are several layers of interoperability, the scope for interoperability addressed in this document is limited to the area of transmission and processing between service providers acting for the trading parties in relation to the transmission and processing of e-Invoices and other electronic business documents as depicted in the diagram below[9]:



6. Model Interoperability Agreement, *supra* note 2, app. 1, at 37.
7. *Id.*
8. Eur. Comm. for Standardization, Conformance Criteria for Interoperability Between Electronic Invoicing Services § 1.2, at 6–7 (May 2012) [hereinafter Conformance Criteria], *available at* ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA16464-3.pdf.
9. *Id.*

Therefore, the "interoperability" envisioned by the Model Interoperability Agreement is similar to common notions of interoperability in the cell phone industry. Each cell phone user may have his or her own carrier and the two carriers have an agreement on how the transmissions are relayed and how the costs are allocated. Similarly, with electronic documents, if each of the trading partners has its own service provider that assists in preparing and formatting the electronic documents, then the Model Interoperability Agreement governs the allocation of responsibilities among those two service providers.[10] With one key exception discussed below relating to confidentiality, the Model Interoperability Agreement governs only the relationship between service providers and does not govern the relationship between those service providers and their (or the other service provider's) customer(s).[11]

When each trading partner has its own service provider, the relationship is referred to as a "four corner" relationship.[12] This contrasts with the situation where each trading partner uses the same service provider (such as a web portal), which is referred to as a "three corner" model or a direct bilateral transmission of documents between trading partners (two corner model).[13] The Model Interoperability Agreement is designed for a four corner model, but many of its principles could be applied in a three or two corner model.[14]

Scope of Model Interoperability Agreement

Section 2.1 of the Model Interoperability Agreement defines its scope as follows:

> The Agreement sets out the terms and conditions for the transmission and processing of e-Invoices and other Electronic Business Documents between the Parties for the purpose that their respective Customers, whether a Sender or a Receiver, shall be able to exchange these documents between each other automatically and without manual intervention. The e-Invoices and Electronic Business Documents to be exchanged and such other services as might be mutually agreed will be specified in the Description of Services. Either or both of SP-X or SP-Y [the two service providers] may act in the capacity of Sending Party and Receiving Party when performing Services under this Agreement.[15]

To make clear that both service providers could be either initiating or receiving a transmission of electronic documents, the Model Interoperability Agreement assigned them the nomenclature of SP-X and SP-Y and specifically avoided the

10. Model Interoperability Agreement, *supra* note 2, at 5 (Preamble).

11. *Id.* "The Parties' relationship with their respective Customers is not regulated and is out of the scope of this Agreement, except as expressly provided in Section 13.7." *Id.* § 3.1, at 6.

12. Eur. Comm. for Standardization, Code of Practice for Electronic Invoicing in the EU 12 (May 2012) [hereinafter Code of Practice], *available at* ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA16463.pdf.

13. *Id.*

14. *See*, *e.g.*, Model Interoperability Agreement, *supra* note 2, § 4, at 7 (Definitions); *id.* § 6, at 10 (Services, Warranty and Service Levels); *id.* § 8, at 12 (Legal and VAT Compliance for e-Invoices); *id.* § 13, at 15 (Confidentiality and Data Protection); *id.* § 16, at 20 (Ownership and Cross License of Data; Intellectual Property Rights); *see also* Conformance Criteria, *supra* note 8, at 8.

15. Model Interoperability Agreement, *supra* note 2, § 2.1, at 6.

terminology of "SP-1" and "SP-2" to minimize any perception that any one service provider's action would always precede the other.[16]

Description of Services Appendix

The Model Interoperability Agreement contains an appendix that specifies the more technical aspects of the transmissions, which is labeled a "Description of Services."[17] This includes such items as the specification of the transport, routing and packaging protocol, the message enveloping and syntax, and what type of acknowledgement will be delivered.[18]

The Appendix serves as a useful checklist for technical issues to be considered whenever sending electronic documents, even for trading partners exchanging them directly without service providers.[19] There are numerous requirements to consider before exchanging documents electronically in a reliable fashion that do not arise in other circumstances, such as the maximum file size, how attachments are handled, and any field requirements, such as maximum number of characters.[20] Failure to anticipate and reach agreement on these details may result in loss of messages or other transmission failures.[21]

Defining Receipt of a Document

The technical aspects of the Description of Services Appendix are woven into the body of the Model Interoperability Agreement and given substantive effect. For example, the definition of when a party receives an electronic document incorporates the requirement that the document was transmitted in accordance with the Description of Services:

> The e-Invoices and Electronic Business Documents that are identified in the Description of Services are deemed to have been transferred to the Receiving Party when the Message containing an e-Invoice or Electronic Business Document is made available to the Receiving Party's system in accordance with the Description of Services and the Sending Party has received a Technical Acknowledgment of receipt. Prior to such receipt, responsibility for the e-Invoice or Electronic Business Document remains with the Sending Party.[22]

Therefore, in order to be able to claim the other party received the document in question, the document must have been transmitted in accordance with the Description of Services.[23]

16. *Id.* § 1.1, at 6.
17. *Id.* app. 1, at 27.
18. *Id.* app. 1, at 28–29.
19. *Id.*
20. *Id.*
21. Eur. Comm. for Standardization, e-Invoicing Compliance Guidelines—Commentary to the Compliance Matrix 32 (Dec. 2009), *available at* ftp://ftp.cen.eu/PUBLIC/CWAs/eInV2/CWA%2016047.pdf.
22. Model Interoperability Agreement, *supra* note 2, § 5.3, at 9.
23. *Id.*

Creating a Trusted Framework

One of the motivations behind the creation of the Model Interoperability Agreement was to accelerate the uptake of electronic invoicing and exchange of electronic documents.[24] While the agreement was aimed at electronic invoicing in the European Union, many of its principles are universal.[25] The authors understood that one of the major inhibitors to sending electronic documents is uncertainty by trading partners regarding the security and confidentiality of their transmissions, especially when those documents are handled by service providers they did not select and who owe them no duties.[26] Trading partners are unlikely to agree to allow another party's service provider to handle their data and view their commercial transactions unless that service provider has made certain assurances regarding how they can use that data.[27]

Therefore, the Model Interoperability Agreement contains numerous provisions that are intended to protect the trading partners, even though the trading partners are not a party to the agreement.[28] Those provisions address the issues and concepts described below.

Confidentiality. The Model Interoperability Agreement contains a fairly typical form of confidentiality agreement, in recognition that the networks will be exchanging pricing and other trade secrets of the trading partners, which the trading partners will expect to remain confidential. The relevant provision is Section 13.1, which provides as follows:

> **Section 13.1—Confidential Information; Limited Disclosure**
>
> The Parties undertake to keep confidential the content of the Agreement, the e-Invoices, Electronic Business Documents and Data, together with all technical, commercial or financial information relating to the other Party, its operations or its Customer that comes to their knowledge. The Parties may, however, disclose to their Customers in general terms that the Agreement exists and include the other Party in a list of entities with whom the Party has interoperability agreements. The Parties may disclose e-Invoices, Electronic Business Documents and their associated Data to such Party's Customer who is the sender or recipient of the e-Invoice or Electronic Business Document. The Parties undertake not to disclose the confidential

24. *Id.* at 5 (Introduction).

25. Conformance Criteria, *supra* note 8, at 8.

26. *See, e.g.*, *Industry Standards for e-Marketplace Participation Agreements*, Nat'l Ass'n of Wholesale Distributors (Aug. 2001) (on file with *The Business Lawyer*); *Good Trading Practices in Electronic Bidding Processes: Reverse Auctions*, Aluminum Foil Container Manufacturers Ass'n (Nov. 2000), http://www.afcma.org/uploads/downloads/AFCMAReverseAuctionPolicy.pdf; *see also NAW Proposes Standards For e-Market Agreements*, Modern Distribution Mgmt. (Aug. 10, 2001), http://www.mdm.com/NAW-proposes-standards-for-e-market-agreements/PARAMS/article/1147.

27. *See supra* note 26.

28. The concept of a trusted framework relates back to recommendations made by the European Union's Expert Group on electronic invoicing. *See* Final Report of the Expert Group on e-Invoicing 7 (Nov. 2009), *available at* http://ec.europa.eu/internal_market/consultations/docs/2009/e-invoicing/report_en.pdf (stating at Recommendation 1.5: "The Expert Group recommends to develop and maintain a competitive and trusted market place for services and solutions and assure trustworthiness and data protection.").

> information referred to above to a third party without a prior written consent from the other Party. If it is necessary for a Party to give its employees or advisers information that is subject to confidentiality, the information may not be disclosed to other persons than those for whom it is necessary to receive such information and who are bound by a confidentiality undertaking either by agreement or by law.[29]

In the portions of the Model Interoperability Agreement governing limits on liabilities, the breach of the confidentiality provision is expressly excluded from any limit on liability and each service provider agrees to accept direct liability to the other service provider's customers even though there is no privity of contract with that customer.[30] This deviates from the general rule of the Model Interoperability Agreement that each service provider only incurs responsibilities and owes duties to its own customers and not the other service provider's customers.[31]

Aggregation of Data. The Model Interoperability Agreement goes one step further than a standard confidentiality clause, however, in recognition that the trading partners own the underlying data. While some confidentiality clauses allow disclosure of information so long as it does not identify a trading partner, the Model Interoperability Agreement bars the disclosure or re-use of the data even in "anonymized" form that does not identify the trading partner. This is because of the fact that the service providers will be handling significant commercial data that can be "data mined" or analyzed easily when in electronic format. Because the trading partners own that data, the networks agree not to make commercial use of the data, or reports based on the data, without the consent of both trading partners. The Model Interoperability Agreement does, however, permit the use of very high levels of aggregated data, so the service providers can, for example, report on the total volume of transactions they handle in a given period of time. The relevant provision is Section 13.2, which provides as follows:

> **Section 13.2—Limited Use and Disclosure of Data**
>
> Each Party agrees not to sell or make commercial use of Data it handles, transmits or stores under this Agreement, except in furtherance of the Services as permitted by this Agreement. The obligations of confidentiality and restrictions on use of Data in this Agreement apply to Data even if it is in anonymous or aggregated form and any works derived from the Data. Notwithstanding the foregoing, each Party may disclose aggregated Data based on all or substantially all of the transmissions it handles during a time period for the purpose of advertising the total volume of transactions or spending handled by its systems during that time period, so long as pricing or other competitively sensitive information of the Customers is not disclosed.[32]

29. Model Interoperability Agreement, *supra* note 2, § 13.1, at 15–16.
30. *Id.* § 14.6, at 19.
31. *Id.* § 3.1, at 6.
32. *Id.* § 13.2, at 16.

This provision was intended to protect the trading partner's data, while allowing the service providers flexibility to advertise the total volume of data they handle on an aggregated basis.[33]

Data License. The Model Interoperability Agreement is structured on the basis that the service providers receive only a limited license to use the trading partner's data. This is intended to provide further protection to trading partners who may be concerned what other uses service providers may make of their data. The relevant provision is Section 16.1, which provides as follows:

> **Section 16.1—Limited License; No Decompilation**
>
> Upon transmission of any Data to a Party by another Party, such Party is thereby granted a revocable, non-exclusive, non-transferable, worldwide, limited license to use the Data in accordance with this Agreement for the sole purposes of performing the Services. In exercising such license, a Party may not use or employ Data for any other purpose or for the benefit of any other party other than Sender and Receiver. A Party may not decompile, disassemble or otherwise reverse engineer the Data or allow any third party to frame or link to the Data.[34]

By structuring the relationship as a license to use the data that is limited to performing the services, any unauthorized use of the data beyond the license terms may, depending on the jurisdiction, create a potential basis for statutory claims against the breaching party for unauthorized access to data or circumventing access controls on the data.[35]

Ownership of Data. Ownership of data is governed by Section 16.2 of the Model Interoperability Agreement, which provides as follows:

> **Section 16.2—Rights to Data**
>
> The Sender and Receiver, jointly or individually, as applicable, retain all rights, title and ownership in the Data and any works derived from the Data. All intellectual property rights associated with the Data, including trade secrets, are retained by the Sender and Receiver, except the limited license to use the Data in performing the Services. Neither the delivery of Data to the Party, nor the conversion of Data by the Party, nor anything else in this Agreement transfers to either Party any ownership or other interest in such Data or any product, device, design, service, process, secret, trademark or anything else described or contained in Data, other than the limited license rights to use the Data as expressly provided in this Agreement.[36]

This provision is intended to provide assurances to each of the ultimate trading partners that no service provider that transmits its data, or any successor of such service provider (such as a bankruptcy trustee), will ever have a basis to claim an ownership interest in the data.[37]

33. *Id.*
34. *Id.* § 16.1, at 20.
35. *See, e.g.*, Real Networks, Inc. v. DVD Copy Control Ass'n, 641 F. Supp. 2d 913 (N.D. Cal. 2009).
36. Model Interoperability Agreement, *supra* note 2, § 16.2, at 20–21.
37. *Id.*

Limits on Fees. The Model Interoperability Agreement addresses fees that may be charged by service providers to the other service provider or that service provider's customers in Section 10.2 (the Model Interoperability Agreement does not address the fees a service provider may charge its own customer):

> **Section 10.2—No Set Up or Professional Fees**
>
> Parties carry all their own costs including development and implementation of the Interoperability Services as well as all on-going maintenance and other costs required during the use of the Interoperability Services.
>
> **Optional Per Transaction Fees**
>
> Any per transaction fees for the Services are set forth in Appendix 1, provided that each Party agrees not to assess to the other Party expenses that are attributable to such Party's own Customers.[38]

This provision is intended to prevent against hidden fees to trading partners by service providers the trading partner did not select.[39] Any fees that one service provider passes on to the other (and which can be expected to be passed on to the trading partner) must be disclosed and agreed to up front.[40] Otherwise, each service provider is responsible for collecting all fees from its own customers—those fees are not regulated or affected by the Model Interoperability Agreement.[41]

Relationship to Other Developments in the European Union Regarding Electronic Invoicing

In July 2010 the European Commission passed "Council Directive 2010/45/EU amending Directive 2006/112/EC on the common system of value added tax as regards the rules of invoicing."[42] The new VAT Directive has the potential to change substantially how electronic commerce and electronic invoicing is performed in the European Union.[43] The member states have until January 1, 2013 to implement national legislation consistent with that new Directive.[44]

Under both the new and the old VAT Directive, electronic invoices may be used so long as the authenticity of the origin (the identity of the sender) and the integrity of the content (no one has altered the invoice in transmission) is demonstrated.[45] The old Directive authorized only two specific technological

38. *Id.* § 10.2, at 14.
39. *Id.*
40. *Id.*
41. *Id.*
42. Council Directive 2010/45/EU, Amending Directive 2006/112/EC on the Common System of Value Added Tax as Regards the Rules on Invoicing, 2010 O.J. (L 189) 1 (EU) [hereinafter VAT Directive], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:189:0001:0008:EN:PDF.
43. *Reaping the Benefits of Electronic Invoicing in the European Union*, COM (2010) 712 final (Dec. 2, 2010), *available at* http://ec.europa.eu/enterprise/sectors/ict/files/com712_en.pdf.
44. VAT Directive, *supra* note 42, art. 2, § 1, at 8.
45. *Compare* Council Directive 2010/45/EU, *supra* note 42, art. 233, at 30, *with* Council Directive 2006/112, art. 233, on the Common System of Value Added Tax, 2006 O.J. (L 347) 1 (EC) [here-

methods of ensuring authenticity of origin and integrity of content: electronic signatures or EDI.[46] The old Directive also allowed member states to permit "other means" to ensure authenticity of origin and integrity of content, but there was little agreement—and much confusion—on what "other means" meant.[47] The new Directive opens the door to a third means, which is the use of "business controls."[48] The business controls used for electronic invoices are intended to be the same as the business controls used for paper, but much discussion remains on how exactly business controls will be applied to electronic invoicing.[49]

In December 2010, the European Commission published a document titled Reaping the Benefits of Electronic Invoicing in the European Union, which called upon CEN to publish a Code of Practice for electronic invoicing.[50] That Code of Practice was intended to provide a framework for member states in transposing the new VAT Directive and to provide a "definition of roles and responsibilities of the distinct actors within the e-invoicing process."[51] The Code of Practice was approved by CEN at the same time as it approved the Model Interoperability Agreement, on February 15, 2012.[52]

Section 3.4 of the Code of Practice calls on service providers who are operating in the "four corner" model to adopt and use the Model Interoperability Agreement.[53] With the full transposition of the new VAT Directive and easier implementation of electronic invoicing in the European Union as a result, it can be expected that the Model Interoperability Agreement will play an ever increasingly important role in governing the transmission of electronic invoices and other business documents in the European Union and in countries trading with the European Union.

inafter Council Directive 2006/112/EC], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:347:0001:0118:en:PDF.

46. Council Directive 2006/112/EC, *supra* note 45, art. 233, at 44.

47. Final Report of the Expert Group on e-Invoicing, *supra* note 28, at 24–25.

48. *Explanatory Notes: VAT Invoicing Rules*, Eur. Comm'n Directorate Gen. Taxation & Customs Union (May 10, 2011), http://ec.europa.eu/taxation_customs/resources/documents/taxation/vat/traders/invoicing_rules/explanatory_notes_en.pdf (Comments).

49. *Id.*

50. *Reaping the Benefits of Electronic Invoicing in the European Union, supra* note 43, at 9 (Action 3.1).

51. *Id.*

52. *See* Code of Practice, *supra* note 12, at 3.

53. *Id.* at 9.

A Survey of Patent Law in Cyberspace

*By Phong Nguyen**

Introduction

Over the past twelve months, the Supreme Court and the Federal Circuit have decided a number of patent cases involving a wide variety of issues. The Supreme Court decided *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*,[1] a particularly important case concerning the patentability of a process doctors can use to determine whether a particular dose of a drug is too high or too low, but at the same time potentially affecting patents in all technology areas, including the internet. The Federal Circuit decided *CyberSource Corp. v. Retail Decisions, Inc.*,[2] a case concerning the patentability of a process and apparatus for determining whether a given online sales transaction is fraudulent. *Leader Technologies, Inc. v. Facebook, Inc.*,[3] also a Federal Circuit decision, addressed whether a prior sale or public use of an invention precluded the inventor from obtaining a patent on the invention. Finally, in *In re Bill of Lading*,[4] the Federal Circuit clarified the pleading requirements for direct and indirect infringement.

Mayo Collaborative Services v. Prometheus Laboratories, Inc.— Unpatentable Subject Matter: Laws of Nature

Section 101 of Title 35 of the United States Code states that "[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor."[5] Although the modifier "any" makes this provision broad,[6]

* Phong D. Nguyen is a partner with Baker Hostetler LLP in its D.C. office where he practices client counseling, patent portfolio procurement, and patent litigation. The author thanks Nilesh Khatri, a summer associate at Baker Hostetler LLP, for his work in helping to summarize cases and edit this survey.

1. 132 S. Ct. 1289 (2012).
2. 654 F.3d 1366 (Fed. Cir. 2011).
3. 678 F.3d 1300 (Fed. Cir. 2012).
4. 681 F.3d 1323 (Fed. Cir. 2012).
5. 35 U.S.C. § 101 (2006).
6. Diamond v. Chakrabarty, 447 U.S. 303, 308 (1980) ("[M]odified by the comprehensive 'any,' Congress plainly contemplated that the patent laws would be given wide scope."); *id.* at 315 (holding that the "patentable subject matter" provisions were broadly stated in order to promote the science and the "useful Arts").

there are judicially created exceptions that prevent patenting laws of nature, natural phenomena, and abstract ideas.[7] However, these exceptions to patentability must have limited scope because fundamentally all inventions rely upon laws of nature, natural phenomena, or abstract ideas.[8] Although laws of nature themselves are not patentable, applications of such laws may be patentable.[9]

Mayo presented the Supreme Court with the question of whether the patentee's claims added enough to rise above descriptions of natural laws to become patent-eligible processes that apply natural laws.[10] In *Mayo*, respondent Prometheus Laboratories, Inc. ("Prometheus") patented a process that doctors could use to determine whether the prescribed dose of thiopurine (a drug used to treat autoimmune diseases) was too low to be effective, or too high, causing harmful side effects in patients.[11] The patent protected the process, which consisted of administering a drug; determining the level of metabolites in the patient's body; comparing that level to the precise levels that determine whether the dose would be ineffective or harmful; and making a decision according to the resulting comparison.[12]

The Supreme Court held that the patent covered a law of nature, that is, the relationship between the concentration of metabolites in the blood and efficacy, rather than an application, of the law.[13] The claims recited three steps: an "administering" step, a "determining" step, and a "wherein" step.[14] Even though these steps are not natural laws, they did not apply the natural law because the process merely told scientists to engage in "well understood, routine, conventional activity already engaged in by the scientific community."[15]

The Supreme Court adhered to controlling precedent, particularly *Diamond v. Diehr* and *Parker v. Flook*.[16] In *Diehr*, the Court upheld the validity of the patent because the steps in the process integrated the law of nature into that process, resulting in an inventive application of the law of nature.[17] On the other hand, the Court rejected the patent in *Flook* because the claimed steps were all "well known" so that when the mathematical formula was removed from the claims, there was no "inventive concept."[18]

As in *Flook*, Prometheus's claims added nothing to the store of knowledge other than the law of nature; in other words, if the law of nature were removed

7. Mayo Collaborative Servs. v. Prometheus Labs., Inc., 132 S. Ct. 1289, 1293 (2012) (citing Diamond v. Diehr, 450 U.S. 175, 180 (1981)).
8. *Id.*
9. *Id.* at 1293–94.
10. *Id.* at 1297.
11. *Id.* at 1294–95.
12. *Id.* at 1295.
13. *Id.* at 1296.
14. *Id.*
15. *Id.* at 1298.
16. *Id.* at 1298–1300 (discussing Diamond v. Diehr, 450 U.S. 175 (1981); Parker v. Flook, 437 U.S. 584 (1978)).
17. *Id.* at 1298–99 (discussing *Diehr*, 450 U.S. at 187–92).
18. *Id.* at 1299 (quoting *Flook*, 437 U.S. at 594).

from the claims, the claims would lack an inventive concept.[19] The remaining portions of the claims simply recited steps that were already well-known, routine, and conventional in the art.[20] Therefore, Prometheus's claims are nothing more than a simple recitation of the law of nature and how to apply it.[21]

The Supreme Court also rejected other arguments by Prometheus and one by the U.S. Government.[22] In response to these arguments, the Court declared that satisfying the machine-or-transformation test does not trump the law-of-nature exclusion.[23] Citing institutional incapacity, the Court rejected an approach that would determine patentability of a law of nature based on how much the patent would interfere with innovation.[24] The Court also rejected the argument that any step beyond a law of nature could be patentable and that other provisions of the Patent Act (such as the nonobvious requirement) would operate to deny unpatentable claims, stating that such an approach would be inconsistent with prior case law and would force other provisions of the Patent Act to do work they were not designed to do.[25] The Court reserved judgment on the impact of its opinion on the incentive system patents create, stating that such a decision was for Congress, not the courts.[26]

Mayo may impact internet-related patents because the Court vacated the judgment in *Ultramercial, LLC v. Hulu, LLC* (commonly known as *WildTangent*, a co-defendant) and remanded the case to the Federal Circuit for reconsideration in light of *Mayo*.[27] The disputed patent in *WildTangent* covered a process that displayed a commercial to an internet user before the user could view copyrighted content.[28] The Federal Circuit originally reversed the district court, holding that the patent covered a patent-eligible process rather than an abstract idea.[29] In light of the *Mayo* decision, the question on remand is likely to focus on whether the invention included a truly inventive step or whether the invention was the work of the patent's draftsperson.

Mayo teaches that inventors and businesses must be mindful of the fact that simply reciting a law of nature wrapped in creative draftsmanship is insufficient to obtain a patent. Rather, the inventor must resourcefully apply the law of nature before obtaining a patent.

19. *Id.* at 1299–1300.
20. *Id.* at 1299.
21. *Id.* at 1299–1300.
22. *Id.* at 1302–05.
23. *Id.* at 1303.
24. *Id.*
25. *Id.* at 1303–04.
26. *Id.* at 1305.
27. Ultramercial, LLC v. Hulu, LLC, 657 F.3d 1323 (Fed. Cir. 2011), *cert. granted sub nom. & vacated*, WildTangent, Inc. v. Ultramercial, LLC, 132 S. Ct. 2431 (2012).
28. *Id.* at 1324.
29. *Id.* at 1330.

CyberSource Corp. v. Retail Decisions, Inc.—Unpatentable Subject Matter: Abstract Ideas

Like *Mayo*, *CyberSource* concerns the scope of patentable subject matter. Rather than a law of nature, the *CyberSource* patent claims an abstract idea.[30] Methods that can be performed in the human mind or with the aid of a pencil and paper, without a connection to other statutory subject matter, are abstract processes and are thus unpatentable.[31] The existence of a practical application for the method does not make the claim patentable because a patent lawyer could add "post-solution activity" to almost any mathematical equation.[32]

In *CyberSource*, the parties disputed the validity of claims two and three of the patent held by CyberSource Corp. ("CyberSource"),[33] which patent was directed to identifying fraud in an online sales transaction.[34] Claim three covered a method comprising three steps: (1) retrieve other internet addresses used with a particular credit card, (2) create a map based upon such information, and (3) use the map to determine if the transaction is fraudulent.[35] Claim two covered a computer readable medium containing instructions to: (1) obtain credit card information related to the transaction, (2) verify such information according to various parameters, and (3) cause the processor to carry out the process of claim three.[36]

The Federal Circuit held that claim three was invalid because it claimed an unpatentable abstract idea.[37] The Federal Circuit held that claim three covered an unpatentable mental process because it was a type of abstract idea—all of the steps could be performed in the human mind or with the aid of a pencil and paper.[38]

The Federal Circuit held claim two invalid as well because it substantially recited nothing more than the process of claim three even though it claimed a computer-readable medium rather than a process.[39] For claim two to be treated as a manufacture claim, rather than a process claim, CyberSource had to prove that the claim is "truly drawn to a specific computer readable medium, rather than to the underlying method."[40] CyberSource was unable to satisfy this burden because a patentee cannot simply make a process that can be entirely accomplished in the human mind patentable merely by having a machine execute the process instead.[41] Therefore, the Federal Circuit held claim two to be a process.[42]

30. CyberSource Corp. v. Retail Decisions, Inc., 654 F.3d 1366, 1371 (Fed. Cir. 2011).
31. *Id.* at 1371–72.
32. *Id.* at 1371 (quoting Parker v. Flook, 437 U.S. 584, 590 (1978)).
33. *Id.* at 1369.
34. *Id.* at 1367–68.
35. *Id.* at 1370.
36. *Id.* at 1373–74.
37. *Id.* at 1371.
38. *Id.* at 1372.
39. *Id.* at 1374.
40. *Id.* at 1375 (internal quotations omitted).
41. *Id.* at 1374–75.
42. *Id.*

Like claim three, claim two claimed an unpatentable mental process. Therefore, the Federal Circuit held claim two invalid.[43]

Businesses must evaluate whether the invented process can be performed completely in the human mind or with the aid of a pencil and paper. If so, the process is likely an abstract mental process and the business would be unable to obtain a patent. Additionally, businesses cannot make an abstract mental process patentable simply by tying it to a machine or another statutory subject matter unless the invention is truly drawn to that machine or another statutory subject matter.

Leader Technologies, Inc. v. Facebook, Inc.—Did the Patentee Jump the Gun?

An invention will be unpatentable if the invention was "in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States."[44] In determining whether the patent is invalid because of a prior public use or sale, the product must have been an embodiment of the claimed invention—that is, it must meet all the limitations of the application's claims.[45] The question before the jury in *Leader* was whether the patentee, Leader Technologies, Inc. ("Leader"), had made its invention unpatentable because Leader had publicly used or offered for sale the invention more than one year prior to filing the patent application.[46]

The disputed patent in *Leader* related to software, named Leader2Leader, which allowed users on large networks to collaborate with each other.[47] The Leader2Leader cofounders, Michael McKibben and Jeffrey Lamb, conceived the idea in 1999 and completed the program in the "2002ish time frame."[48] In January 2002, Leader presented a white paper to an Air Force base, and, in December 2002, Leader offered the product for sale to a handful of other companies.[49] On December 11, 2002, Leader filed a provisional patent application, and, on December 10, 2003, Leader filed the corresponding nonprovisional patent application that would issue as the disputed patent.[50]

Leader sued Facebook in 2008 for infringing its patent.[51] When Facebook deposed McKibben, he testified that he could not remember any version of Leader2Leader that did not fall within the patent claims.[52] However, at trial McKibben testified to "vividly remember[ing]" that the patented technology was not incorporated into the software "until days before" the provisional patent

43. *Id.* at 1376–77.
44. 35 U.S.C. § 102(b) (2006).
45. Leader Techs., Inc. v. Facebook, Inc., 678 F.3d 1300, 1305 (Fed. Cir. 2012).
46. *Id.* at 1304–05.
47. *Id.* at 1301–02.
48. *Id.* at 1302–03.
49. *Id.* at 1303.
50. *Id.* at 1304.
51. *Id.*
52. *Id.*

application.[53] The critical date is one year prior to the filing of the patent application;[54] in this case, it was December 10, 2002. The jury found that the patent was invalid because the invention had been sold and it was publicly used before the critical date, i.e., more than one year before the nonprovisional application filing date.[55]

The Federal Circuit held that there was legally sufficient evidence to support the jury's conclusion that Leader's product was on sale or in public use before the critical date and that it met the limitations of the claimed invention.[56] The Federal Circuit cited McKibben's deposition as supporting evidence that Leader2Leader had always been covered by the patent.[57] Additionally, Leader's statements to its customers that Leader was selling them a "fully developed" version of the software lent additional weight to the jury's finding that Leader had sold its invention prior to the critical date.[58] Thus, because Leader had sold and publicly used the invention prior to the critical date, Leader was estopped from obtaining a patent on the Leader2Leader software.[59]

The *Leader* case illustrates how careful businesses must be when timing patent applications. The business must file a patent application within one year of publicly demonstrating or offering for sale the invention. Otherwise, the business will be unable to obtain patent protection on the invention.

In re Bill of Lading—Pleading Requirements for Infringement

Upon their adoption in 1937, the Federal Rules of Civil Procedure relaxed the pleading requirements, with Rule 8(a)(2) requiring the plaintiff to include only a "short and plain statement of the claim showing that the pleader is entitled to relief."[60] The Supreme Court, however, seemingly elevated the pleading requirements in the recent decisions of *Ashcroft v. Iqbal* and *Bell Atlantic Corp. v. Twombly*.[61]

A patent plaintiff may claim either direct infringement or indirect infringement, which includes contributory infringement and induced infringement.[62] To succeed on a claim of indirect infringement, the patentee must first show that there was direct infringement.[63]

53. *Id.*

54. 35 U.S.C. § 102(b) (2006).

55. *Leader Techs., Inc.*, 678 F.3d at 1304. The district court denied Leader's post-trial motions for judgment as a matter of law and for a new trial. *Id.* Leader appealed those denials. *Id.* at 1305.

56. *Id.* at 1306–08.

57. *Id.* at 1306.

58. *Id.* at 1307.

59. *Id.* at 1308.

60. Fed. R. Civ. P. 8(a)(2); *see* Fed. R. Civ. P. 8 advisory committee's notes; Charles E. Clark, *Simplified Pleading*, 2 F.R.D. 456, 463 (1943).

61. Ashcroft v. Iqbal, 556 U.S. 662, 680 (2009) (requiring plaintiff to plead plausible, not just conceivable, facts); Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007) (same); *compare* Conley v. Gibson, 355 U.S. 41, 45–46 (1957) ("[T]he accepted rule [is] that a complaint should not be dismissed for failure to state a claim unless it appears beyond doubt that the plaintiff can prove no set of facts in support of his claim . . . .").

62. *In re* Bill of Lading, 681 F.3d 1323, 1333 (Fed. Cir. 2012) (citing Dynacore Holdings Corp. v. U.S. Philips Corp., 363 F.3d 1263, 1272 (Fed. Cir. 2004)).

63. *Id.*

In *In re Bill of Lading*, R+L Carriers, Inc. ("R+L") held the disputed method patent which increases the efficiency for the less-than-a-load trucking industry by wirelessly sending shipping documents from the truck to a central facility so that load planning can occur while the load is in transit.[64] R+L brought direct and indirect infringement claims against the defendants.[65] The district court granted the defendants' Rule 12(b)(6) motion because R+L had failed to meet the pleading requirements set forth by *Iqbal* and *Twombly*.[66]

On appeal, the Federal Circuit addressed: (1) whether a party is liable for contributory infringement for an offer to sell a patented method, and (2) whether direct infringement is necessary for contributory infringement based upon such an offer to sell.[67] The Federal Circuit answered both questions in the affirmative.[68] The court found that R+L adequately pleaded direct infringement.[69] Form 18, located in the Federal Rules of Civil Procedure Appendix of Forms, governs some parts of a patent infringement claim and requires five simple elements.[70] Such forms are relevant in determining whether a plaintiff has met the pleading standard because they illustrate "the simplicity and brevity" the Rules contemplate.[71] Additionally, the Supreme Court has stated that the Federal Rules can be changed only through an amendment process, not through judicial interpretation.[72] Therefore, when case law regarding pleading requirements conflicts with requirements established by the forms, the forms govern.[73] As a result, if R+L met the requirements of Form 18, then R+L also met the pleading requirements for a direct infringement claim.[74] Here, R+L's pleading was sufficient for a direct infringement claim for those claims that pleaded a specific infringer.[75] However, in certain pleadings, R+L was unable to name a specific infringer; instead, it alleged infringement only by those customers practicing the patent.[76] Relying on its precedent, the Federal Circuit held that, to plead direct infringement for purposes of indirect infringement, the patentee need not identify a specific direct infringer but must allege facts that give rise to a reasonable inference that there is at least one direct infringer.[77] Here, because R+L alleged sufficient facts for purposes of Form 18, R+L satisfied its pleading requirements for direct infringement.[78]

64. *Id.* at 1329.
65. *Id.*
66. *Id.* at 1330–31.
67. *Id.* at 1333.
68. *Id.*
69. *Id.*
70. *See id.* at 1334 (discussing FED. R. CIV. P. form 18).
71. *Id.* (quoting FED. R. CIV. P. 84).
72. *Id.* (citing Bell Atl. Corp. v. Twombly, 550 U.S. 544, 569 n.14 (2007)).
73. *Id.*
74. *Id.*
75. *Id.* at 1335.
76. *Id.* at 1336.
77. *Id.* (citing, *inter alia*, Lucent Techs., Inc. v. Gateway, Inc., 580 F.3d 1301, 1318 (Fed. Cir. 2009)).
78. *Id.*

Because Form 18 applies only to direct infringement claims, the Federal Circuit looked to Supreme Court precedent to determine whether R+L had adequately pleaded contributory and induced infringement.[79] To adequately plead contributory infringement, the plaintiff must allege, among other things, sufficient facts that allow an inference that the components sold or offered for sale have no substantial non-infringing uses.[80] Here, R+L alleged facts in its complaint that defeated its contributory infringement claim because R+L referenced many other possible uses of the defendants' products.[81]

To survive the defendants' motion to dismiss the induced infringement claims, R+L must have alleged facts plausibly showing that the defendants intended their customers to infringe the patent and that the defendants knew that their customers' acts would constitute infringement.[82] Here, R+L's induced infringement claims survived the defendants' motion to dismiss because, when drawing all reasonable inferences in R+L's favor and considering the context and technology of the industry, R+L had plausibly pleaded induced infringement against all of the defendants.[83]

This case illustrates the ease with which a plaintiff can plead a direct patent infringement case and the difficulty a defendant faces in dismissing such a case. Form 18's requirements are not demanding and thus not very difficult for a plaintiff to plead adequately. However, claims for contributory infringement and induced infringement must meet the pleading requirements set forth by *Iqbal* and *Twombly*.

Conclusion

The last year has seen important cases concerning the patentability of inventions, the most important being *Mayo*, in which the Court held that the patent simply covered a law of nature, which is unpatentable, rather than an application of a law of nature, which could be patentable. Additionally, simply gathering and organizing information with a computer—a task that could be accomplished entirely in the human mind or with the aid of a pencil and paper—are mental processes and unpatentable because they are abstract ideas. If an invention that meets all of the claim limitations is on sale or in public use more than one year before the patent application's filing date, the inventor will be estopped from obtaining a patent on that invention. Finally, if a plaintiff conforms with the requirements of Form 18 for a direct infringement claim, then a defendant cannot successfully move to dismiss it pursuant to Rule 12(b)(6). However, if a plaintiff brings a claim for indirect infringement, then the plaintiff must meet the elevated pleading requirements of *Iqbal* and *Twombly*.

79. *Id.* at 1337.
80. *Id.*
81. *Id.* at 1338.
82. *Id.* at 1339.
83. *Id.* at 1340.

2012 State of the Law Regarding Internet Intermediary Liability for User-Generated Content

*By Catherine R. Gellis**

I. Introduction

Of the two major statutes that largely govern intermediary liability for user-generated content—47 U.S.C. § 230 ("Section 230")[1] and 17 U.S.C. § 512 (the "DMCA")[2]—the most significant updates from the past year have centered on the latter, particularly with two important appellate rulings regarding video-hosting sites. But jurisprudence surrounding Section 230 has also continued to solidify, with some notable updates as well.

II. 47 U.S.C. § 230 Updates

Section 230, by design, does most of the heavy lifting regarding intermediary liability for user-generated content, preempting most state laws[3] and covering most types of liability.[4] Subsection (c)(1) is key: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[5] In other words, while the nature of the content may raise questions of legal liability, only the *user* who posted the content can be held liable for it, not the website hosting it.[6]

This statutory prohibition has not kept plaintiffs from trying to hold the web hosts liable anyway, but most of their efforts have been ill-fated.[7] For instance,

* Ms. Gellis is a former internet professional turned internet lawyer in the San Francisco Bay Area. B.A. Mass Communications and Sociology, University of California, Berkeley; J.D. Boston University. As is becoming well-deserved custom, the author once again thanks Eric Goldman for his invaluable Technology & Marketing Law Blog.

1. 47 U.S.C. § 230 (2006).

2. 17 U.S.C. § 512 (2006 & Supp. IV 2010). Section 512 was enacted as part of the Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

3. 47 U.S.C. § 230(e)(3).

4. *See* 47 U.S.C. § 230(e)(1), (2), (4).

5. 47 U.S.C. § 230(c)(1).

6. Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008) ("Section 230 of the CDA immunizes providers of interactive computer services against liability arising from content created by third parties.").

7. *See*, *e.g.*, Riggs v. MySpace, Inc., 444 F. App'x 986, 987 (9th Cir. 2011); Hopkins v. Doe #1, No. 2:11-CV-100-RWS, 2011 WL 5921446, at *2 (N.D. Ga. Nov. 28, 2011). In *Shrader v. Biddinger*, the web host was deemed eligible for an award of attorney's fees under the Colorado statute that normally

like courts have ruled in previous years, recent rulings have affirmed that newspapers cannot be held responsible for comments readers post on their websites.[8] Similarly Facebook, Google, and LexisNexis were dismissed from lawsuits trying to hold them accountable for content appearing on their systems that other people had created.[9] Note, though, that it is not just web hosts that are entitled to this immunity; the statute covers "interactive computer service provider[s]," meaning "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server."[10] Thus in *Holomaxx Technologies Corp. v. Microsoft Corp.*[11] and *Holomaxx Technologies Corp. v. Yahoo! Inc.*,[12] e-mail providers were also deemed interactive computer service providers eligible for the protections of the statute.

Ultimately, if the content at issue was not produced by the interactive computer service provider, the provider should be immune no matter what sort of liability the content itself might incur.[13] Section 230 should even allow the provider to get out of a lawsuit based on user-generated content on a motion to dismiss.[14] But sometimes courts hesitate and allow the trial to continue in order to determine whether the host was truly an immune service provider or, rather, so closely connected with the actual development of the content as to be considered the non-immune information content provider instead.[15]

This delay can be unfortunate, however, as it can make it very expensive for the host to ultimately receive the immunity the statute intended to provide it.[16] This point was driven home by a recent Ninth Circuit ruling in *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*.[17] In 2008, an earlier ruling by the same court in the same case became one of the seminal pieces of Section 230 jurisprudence. In that decision the Roommates.com website was entitled to Section 230 immunity with respect to the free form content users provided in the roommate ads they posted but *not* for the supposedly illegal

allows for fee recovery for a dismissed tort claim. No. 10-cv-01881-REB-MJW, 2012 WL 976032, at *17 (D. Colo. Feb. 17, 2012).

8. *See*, *e.g.*, Spreadbury v. Bitterroot Pub. Library, No. CV 11-64-M-DWM-JCL, 2012 WL 734163, at *1–2 (D. Mont. Mar. 6, 2012); *see also* Delle v. Worcester Telegram & Gazette Corp., No. 110810, 2011 WL 7090709, at *4 (Mass. Super. Ct. Sept. 14, 2011).

9. Gaston v. Facebook, Inc., No. 3:12-cv-0063-ST, 2012 WL 629868, at *7 (D. Or. Feb. 2, 2012) (finding Facebook, Google, and LexisNexis not liable for hosting content created by someone else), *report & recommendation adopted by* No. 3:12-cv-00063-ST, 2012 WL 610005 (D. Or. Feb. 24, 2012); *see also* Black v. Google, Inc., 457 F. App'x 622 (9th Cir. 2011).

10. 47 U.S.C. § 230(f)(2).

11. No. 10-cv-04924 JF (HRL), 2011 WL 3740813, at *2–3 (N.D. Cal. Aug. 23, 2011).

12. No. 10-cv-04926 JF (PSG), 2011 WL 3740827, at *2 (N.D. Cal. Aug. 23, 2011).

13. *See* Inman v. Technicolor USA, Inc., No. 11-666, 2011 WL 5829024, at *6–7 (W.D. Pa. Nov. 18, 2011) (finding that Section 230 kept eBay from being liable for the defects in products sold by a user).

14. *See*, *e.g.*, Price v. Gannett Co., No. 2:11-cv-00628, 2012 WL 1570972, at *2 (S.D. W. Va. May 1, 2012).

15. *See*, *e.g.*, Chang v. Wozo LLC, No. 11-10245-DJC, 2012 WL 1067643, at *14 (D. Mass. Mar. 28, 2012); Wang v. OCZ Tech. Grp., Inc., 276 F.R.D. 618, 631–32 (N.D. Cal. 2011).

16. *See* Giordano v. Romeo, 76 So. 3d 1100, 1102 (Fla. Dist. Ct. App. Dec. 28, 2011) (affirming the host's entitlement to its long-delayed immunity).

17. 666 F.3d 1216 (9th Cir. 2012).

discriminatory preferences the site prompted users to enter along with it as part of their ads.[18] Per the court, it was that illegality itself that justified the loss of the immunity.[19] But because the same court found in its recent ruling that discriminatory preferences in shared housing offers ultimately did not violate fair housing law after all, the rationale for having originally denied the immunity appears to have been undermined.[20]

Ordinarily, however, immunity will not be lost just because the host may have interacted with the content at issue in some way.[21] In *Levitt v. Yelp! Inc.*, the district court also found that the possible intent of the host in making edits was irrelevant.[22] While subsection (c)(2) of Section 230 creates a separate immunity for a host's "good faith" filtering of content transmitted through its systems by users,[23] subsection (c)(1) requires no similar good faith requirement for a host to be eligible for the immunity.[24] On the other hand, in *Vo Group, LLC v. Opinion Corp.*, the court denied the defendant's motion to dismiss on Section 230 grounds by imputing that the website might have become the non-immune creator of ostensibly defamatory user-generated content when it tried to charge to have it removed.[25] And in *Jones v. Dirty World Entertainment Recordings*, the same website in question was denied Section 230 protection for similar reasons.[26]

18. Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1165, 1174–75 (9th Cir. 2008).

19. "[Roommates.com] is being sued for the predictable consequences of creating a website designed to solicit and enforce housing preferences that are alleged to be illegal." *Id.* at 1170.

20. *Roommates.com*, 666 F.3d at 1222. Notably, in its earlier ruling the court had also held that "section 230 must be interpreted to protect websites not merely from ultimate liability, but from having to fight costly and protracted legal battles." *Fair Hous. Council*, LLC, 521 F.3d at 1175.

21. *See* Shiamili v. Real Estate Grp. of N.Y., Inc., 17 N.Y.3d 281, 289 (2011) (finding Section 230 bars "lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone, or alter content"); *see also id.* at 291–92; Deer Consumer Prods., Inc. v. Little, No. 650823/11, 2011 WL 4346674 (N.Y. Sup. Ct. Aug. 31, 2011); A-1 Tech., Inc. v. Magedson, No. 150033/10, slip op. at 9–10 (N.Y. Sup. Ct. June 22, 2011), *available at* http://scribd.com/doc/58850590/A-1-Technology-Inc-v-Ed-Magedson-Order-Granting-Motion-to-Dismiss.

22. Nos. C-10-1321 EMC, C-10-2351 EMC, 2011 WL 5079526, at *7–8 (N.D. Cal. Oct. 26, 2011) (finding that reordering reviews did not compromise Yelp's immunity).

23. 47 U.S.C. § 230(c)(2) (2006) ("No provider or user of an interactive computer service shall be held liable on account of . . . any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable . . . ."); *see* Holomaxx Techs. Corp. v. Microsoft Corp., No. 10-cv-04924 JF (HRL), 2011 WL 3740813, at *2 (N.D. Cal. Aug. 23, 2011) (applying 47 U.S.C. § 230(c)(2) to filtering for spam); Holomaxx Techs. Corp. v. Yahoo! Inc., No. 10-cv-04926 JF (PSG), 2011 WL 3740827, at *2 (N.D. Cal. Aug. 23, 2011) (same). *But see* Google, Inc. v. MyTriggers.com, Inc., No. 09CVH10-14836, slip op. at 7 (Franklin Cnty. Ct. Com. Pl. Aug. 31, 2011), *available at* http://www.scribd.com/doc/63751818/Google-v-MyTriggers-Dismissal (narrowly construing the type of filtering of "objectionable" content to which subsection (c)(2) immunity applies).

24. *Levitt*, 2011 WL 5079526, at *7.

25. No. 8758/11, slip op. at 1, 5 (N.Y. Sup. Ct. May 22, 2012), *available at* http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1073&context=historical. By contrast, in *Ascentive, LLC v. Opinion Corp.*, the same website was deemed Section 230-eligible. No. 10 Civ. 4433 (ILG) (SMG), 2011 WL 6181452, at *21 (E.D.N.Y. Dec. 13, 2011).

26. No. 09-219-WOB, 2012 WL 70426, at *4 (E.D. Ky. Jan. 10, 2012).

Citing *FTC v. Accusearch Inc.*,[27] the court in *Jones* held that "[a] service provider is 'responsible' for the development of offensive content only if it in some way specifically encourages the development of *what is offensive about the content*."[28] But in that case, "[through] the very name of the site, the manner in which it is managed, and the personal comments of [the site owner]," the court decided it did.[29]

Yet in *S.C. v. Dirty World, LLC*, the court found that the same website was entitled to the immunity.[30] Criticizing the earlier *Jones* ruling, the court said that content development required a *material contribution* to the alleged illegality; mere "encouragement" of its development would not be enough to waive immunity.[31] Similarly, in another case involving potentially salacious content, the Village Voice's Backpage.com site was able to avoid liability for sex trafficking as a result of hosting online ads of apparently suspect escort services.[32] Meanwhile in *Hill v. StubHub, Inc.*, the appeals court affirmed that user-generated content is user-generated content, and that all liability for it—in this case for violation of anti-scalping laws—belonged with the users who had created it, not with the host that had simply intermediated it.[33]

III. 17 U.S.C. § 512 Updates

Subsection (e)(2) exempts "intellectual property" from Section 230's purview, meaning that web hosts cannot use that statute to insulate themselves from IP infringements in their users' content.[34] When it comes to copyright liability, however, as long as they comply with the statute's requirements, hosts can avail themselves of the safe harbors of the Digital Millennium Copyright Act ("DMCA"), codified at 17 U.S.C. § 512, to insulate themselves from the consequences of that infringement.[35] The requirements most applicable to Section 230-eligible intermediaries are those found at subsection (c) addressing

27. 570 F.3d 1187, 1190 (10th Cir. 2009).

28. 2012 WL 70426, at *3.

29. *Id.* at *5.

30. No. 11-CV-00392-DW, slip op. at 9–10 (W.D. Mo. Mar. 12, 2012), *available at* http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1017&context=historical.

31. *Id.* at 5–6. The same website was also able to avoid liability in *Gauck v. Karamian*, 805 F. Supp. 2d 495, 503 (W.D. Tenn. 2011) and *Dyer v. Dirty World, LLC*, No. CV-11-0074-PHX-SMM, 2011 WL 2173900, at *3 (D. Ariz. June 2, 2011). In these cases, however, the findings of no liability were based on the courts' conclusions that the defendants had not violated the plaintiffs' rights of publicity and privacy, respectively, and not because of Section 230. *Gauck*, 805 F. Supp. 2d at 503; *Dyer*, 2011 WL 2173900, at *3.

32. M.A. v. Vill. Voice Media Holdings, LLC, 809 F. Supp. 2d 1041, 1058 (E.D. Mo. 2011). The immunity withstood all the plaintiff's challenges, including that Backpage.com profited from the ads it allowed users to post, that the site knew about the content of those ads, and that the underlying illegality of the ads was based on criminal law. *Id.* at 1050–51, 1054–55.

33. No. COA11-685, 2012 WL 696223, at *13 (N.C. Ct. App. Mar. 6, 2012).

34. 47 U.S.C. § 230(e)(2) (2006).

35. It is an open question, however, whether the safe harbor applies to *state* copyright claims. *See* Capitol Records, Inc. v. MP3tunes LLC, 821 F. Supp. 2d 627, 640–42 (S.D.N.Y. 2011) (finding the safe harbor provision does apply to state copyright claims). *But see* U.S. Copyright Office, Federal Copyright Protection for Pre-1972 Sound Recordings 130–32 (2011), *available at* http://www.copyright.gov/docs/sound/pre-72-report.pdf (reaching the opposite conclusion).

internet service providers that host "information residing on [their] systems or networks at [the] direction of users."[36]

Two significant appellate cases handed down recently clarify what those requirements are and when a web host could be deemed eligible for the safe harbor: *UMG Recordings, Inc. v. Shelter Capital Partners LLC*,[37] from the Ninth Circuit, and *Viacom International, Inc. v. YouTube, Inc.*,[38] from the Second Circuit, which was rendered a few months afterward. In addition to both defendants being sites that hosted user-posted videos (Veoh Networks and YouTube, respectively),[39] the cases also share certain commonalities in their rulings but diverge in at least one key way.

The first point of convergence centers around what it means to host content stored at the direction of users. As the court noted in *Shelter Capital*, Veoh automatically converted the video files users uploaded, but this conversion did not change the fact that ultimately the content still came to reside on its systems at the direction of users.[40] In *Viacom*, the court reached a similar conclusion, although it remanded the case for more fact-finding to determine if the syndication element of the YouTube site was consistent with § 512(c)(1).[41]

The safe harbor also will not apply if the service provider has "actual knowledge" of infringing content on its systems, or an awareness of "facts or circumstances" from which it should realize there is infringing content, and then does not "act[] expeditiously to remove, or disable access to, the material."[42] The plaintiff in *Shelter Capital* had argued that because Veoh was hosting music videos, and because it knew it had no license to host music videos, it therefore should have known it was hosting infringing content and thus should have acted immediately to delete it.[43] But the court disagreed, referring back to earlier cases and the statute that make it clear the host has no obligation to police for infringing content on its site.[44] Particularly because some content, including music videos, could be there legitimately, only the rights owner is able to truly know whether there is infringing content or not.[45] The *Viacom* court meanwhile reached a similar conclusion, noting that the removal obligation could only work in the face of specific knowledge of what to remove.[46]

The service provider is furthermore only eligible for the safe harbor if it "does not receive a financial benefit directly attributable to the infringing activity, in a

36. 17 U.S.C. § 512(c)(1) (2006).
37. 667 F.3d 1022 (9th Cir. 2011).
38. 676 F.3d 19 (2d Cir. 2012).
39. *Shelter Capital*, 667 F.3d at 1026; *Viacom*, 676 F.3d at 25.
40. *Shelter Capital*, 667 F.3d at 1035 ("Veoh does not actively participate in or supervise file uploading . . . . Rather, this 'automated process' for making files accessible 'is initiated entirely at the volition of Veoh's users.' " (internal citations omitted)).
41. *Viacom*, 676 F.3d at 38–39.
42. 17 U.S.C. § 512(c)(1)(A)(i)–(iii) (2006).
43. *Shelter Capital*, 667 F.3d at 1036.
44. *Id.* at 1037–38 (citing 17 U.S.C. § 512(m); Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1113 (9th Cir. 2007)).
45. *Shelter Capital*, 667 F.3d at 1036.
46. *Viacom*, 676 F.3d at 30.

case in which the service provider has the right and ability to control such activity,"[47] but here is where the two courts diverged. The *Shelter Capital* court held that "the 'right and ability to control' . . . requires control over specific infringing activity the provider knows about. A service provider's general right and ability to remove materials from its services is, alone, insufficient."[48] But the *Viacom* court specifically rejected this view on statutory construction grounds.[49] Nonetheless, it left it to the lower court to determine based on the record whether YouTube complied with this requirement, without articulating further what the requirement entailed.[50]

The safe harbor requirements include a few other criteria, such as the need for a service provider to have a repeat infringer policy and not to interfere with "standard technical measures,"[51] considerations the *Viacom* court quickly dispensed with by citing to previous precedent[52] and the *Shelter Capital* court only touched on in a footnote.[53] In another recent case, however, a court found that providing tools enabling watermarks to be removed from pictures did not disqualify the host for failing to "comply with standard technical measures."[54] That same case also spoke to the role that takedown notices played in conveying knowledge of infringement to the service provider.[55] The copyright owner could not simply send a few and then presume the service provider would police their systems from there; rather the copyright owner had to continue to send specific takedown notices identifying where each infringement was located.[56]

IV. Conclusion

Ultimately these two statutes, 47 U.S.C. § 230 and 17 U.S.C. § 512, are increasingly providing clarity and protection to internet intermediaries hosting user-generated content, albeit with a few inconsistencies along the way. What is unclear, however, is how much they may matter in the future. While their jurisprudence continues to evolve, other forces are at work reshaping the terrain for intermediaries. For instance, this past year Congress nearly passed bills that would have displaced much of the DMCA and potentially put hosts in a position

47. 17 U.S.C. § 512(c)(1)(B) (2006).
48. *Shelter Capital*, 667 F.3d at 1043.
49. *Viacom*, 676 F.3d at 37.
50. *Id.* at 38 ("[W]e conclude that the 'right and ability to control' infringing activity under § 512(c)(1)(B) 'requires something more than the ability to remove or block access to materials posted on a service provider's website.' The remaining—and more difficult—question is how to define the 'something more' that is required." (internal citations omitted)).
51. 17 U.S.C. § 512(i)(1) (2006).
52. *Viacom*, 676 F.3d at 40–41.
53. *Shelter Capital*, 667 F.3d at 1031 n.5.
54. Wolk v. Kodak Imaging Network, Inc., No. 10 Civ. 4135, 2012 WL 11270, at *18 (S.D.N.Y. Jan. 3, 2012).
55. *Id.* at *20–21.
56. *Id.*

to police, and therefore censor, their users' content.[57] We also have seen the seizure of websites and domain names,[58] a practice that inherently pressures intermediaries hosting user content. These and other such efforts may ultimately have more impact on intermediaries than anything the courts might decide regarding 47 U.S.C. § 230 and 17 U.S.C. § 512, the two statutes discussed above.

57. *See*, *e.g.*, Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011); Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968, 112th Cong. (2011).

58. *See*, *e.g.*, *In re* Seizure of rapgodfathers.com, torrent-finder.com, rmx4u.com, dajazi.com & onsmash.com, No. 10-2822M (C.D. Cal. Nov. 24, 2010), *available at* https://www.eff.org/node/70613; Mike Masnick, *Judge Lets Feds Censor Blog for Over a Year so the RIAA Could Take Its Sweet Time*, TechDirt (May 3, 2012), http://www.techdirt.com/articles/20120502/16575418746/.

A Survey of False Advertising in Cyberspace

*By Cheryl Dancey Balough**

As the internet plays a more important role in marketing, false advertising claims that target companies' use of websites and social media continue to grow. Key cases from mid-2011 through mid-2012 evidence this phenomenon and introduce some new variations to false advertising claims. These cases include claims related to blog posts, pseudonymous online reviews, cybersquatting, and mobile applications.

The Lanham Act provides that:

> Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which . . . (B) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities, shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.[1]

False advertising complaints may also be filed under state statutes.[2]

I. Claims Against Competitors

Recent false advertising cases of note include claims that competitors made false statements on their websites that misled potential customers. One such case involved two former partners in a company called McLane Associates, Inc. who separated and subsequently competed for management services projects.[3] McGrath accused PCM of false advertising, alleging that PCM's website included false statements that gave the impression PCM was a larger, more experienced company than it was.[4] McGrath said the website statements were literally false because they reported for PCM data that was actually the combination

* Cheryl Dancey Balough is a principal of Chicago-based Balough Law Offices, LLC. She serves as communications co-director of the Cyberspace Law Committee of the ABA Section of Business Law.

1. Lanham Act § 43, 15 U.S.C. § 1125(a)(1) (2006).

2. *See, e.g.*, Cal. Bus. & Prof. Code §§ 17500–17606 (West 2012); *id.* §§ 17200–17210, 17500–17850 (West 2008 & Supp. 2011).

3. McGrath & Co. v. PCM Consulting, Inc., 2012 U.S. Dist. LEXIS 18584, at *2–4 (D. Mass. Feb. 15, 2012).

4. *Id.* at *6–7.

of PCM's data with McLane data, thereby intentionally misleading potential customers.[5]

The court denied PCM's motion to dismiss, finding that McGrath adequately stated a claim for false advertising. To state such a claim under the Lanham Act, a plaintiff must allege that:

> (1) the defendant made a false or misleading description of fact or representation of fact in a commercial advertisement about his own or another's product; (2) the misrepresentation is material, in that it is likely to influence the purchasing decision; (3) the misrepresentation actually deceives or has the tendency to deceive a substantial segment of its audience; (4) the defendant placed the false or misleading statement in interstate commerce; and (5) the plaintiff has been or is likely to be injured as a result of the misrepresentation, either by direct diversion of sales or by a lessening of goodwill associated with its products.[6]

The court specifically noted that McGrath's complaint adequately alleged that PCM's website statements constituted commercial advertising because they promoted PCM's services to any consumer who viewed the website.[7] The misrepresentations were material because they could influence prospective clients.[8] Furthermore, when "one operates a website containing alleged false or misleading statements, the party causes those statements to enter interstate commerce through the internet."[9] While the *McGrath* court explained how the PCM website met the criteria for false advertising, other courts assume that website content is commercial advertising that is both material and interstate in nature, much like television promotion and product packaging.[10]

Another recent case, *iYogi Holding PVT Ltd. v. Secure Remote Support, Inc.*,[11] addressed false or misleading content that a company posted on its website blog about a direct competitor, as well as shill reviews. iYogi's complaint, to which Secure Remote Support, Inc. ("SRS") did not respond, alleged that SRS's website blog contained false, misleading, and defamatory statements about iYogi and a hyperlink to "iyogireviewsonline.com," a site containing similar statements.[12] SRS owned and operated the latter website, although the site did not indicate any connection to SRS.[13] iYogi further alleged that SRS "intentionally published false, misleading and defamatory reviews, testimonials and comments regarding Plaintiff's services on other consumer websites (without disclosing the fact that the authors of these negative comments have a material connection with SRS . . .)."[14] The magistrate judge found that iYogi adequately pled false advertising, under both the

5. *Id.*
6. *Id.* at *8 (quoting Cashmere & Camel Hair Mfrs. Inst. v. Saks Fifth Ave., 284 F.3d 302, 310–11 (1st Cir. 2002)).
7. *Id.* at *10.
8. *Id.* at *15.
9. *Id.* at *17.
10. *See, e.g.*, CJ Prods. L.L.C. v. Snuggly Plushez L.L.C., 809 F. Supp. 2d 127, 146–48 (E.D.N.Y. 2011).
11. 2011 U.S. Dist. LEXIS 144425 (N.D. Cal. Oct. 25, 2011).
12. *Id.* at *3–4.
13. *Id.* at *4.
14. *Id.* at *5.

Lanham Act and California's False Advertising Law, and recommended that iYogi's motion for default judgment and request for an injunction be granted, which the district court adopted.[15]

In some recent contested cases, however, courts have been more reticent to conclude that blog posts or reviews posted under pseudonyms contain literally false or misleading statements that constitute false advertising. In *QVC, Inc. v. Your Vitamins, Inc.*,[16] an appellate court affirmed the lower court's denial of a preliminary injunction against publication of a competitor's blog posts. After Your Vitamins moved promotion of its Healthy Hair, Skin, and Nails product from QVC to QVC's rival HSN, QVC introduced an identically named product.[17] Your Vitamins' owner, Lessman, then posted blog comments on his website complaining about QVC's conduct, alleging that QVC's product is over 90 percent additives, that "there is a significant body of troubling research that connects hyaluronic acid, an ingredient in QVC's [product], to cancer," and that "it is totally useless and potentially harmful."[18] The blog posts expressed similar concerns about two other QVC products and called QVC products " 'ridiculous,' 'embarrassing,' 'sad,' and 'disturbing.' "[19]

The court found that Lessman's posts were not literally false.[20] As to whether the posts were misleading, the court stated that "where the advertisements are not literally false, plaintiff bears the burden of proving actual deception by a preponderance of the evidence. . . . [I]t must show how consumers *actually* do react."[21] The court found that the only evidence of consumer reaction to Lessman's posts were about sixty comments "purportedly left by consumers" and that "only a handful suggested that consumers had been misled into a materially false belief about QVC's products."[22] Moreover, the court stated that blog post comments should be given only limited weight because they "can be very difficult to authenticate" given the popular use of false identities in internet forums to attack corporate rivals and, "[e]ven if a poster is 'legitimate,' doubts will often remain as to the sincerity of the comment."[23]

In *Boykin Anchor Co. v. AT&T Corp.*,[24] the court granted AT&T's motion to dismiss Boykin's false advertising claim because the internet postings at issue were not a commercial advertisement or other promotion. Boykin Anchor competed with just one company, Hilti, for AT&T's purchase of seismic anchors.[25] An AT&T employee, Wong, whose advice impacted what products, including

15. *Id.* at *6, *41–44, *57–58; *see also* iYogi Holding PVT Ltd. v. Secure Remote Support, Inc., 2011 U.S. Dist. LEXIS 144413 (N.D. Cal. Dec. 15, 2011).
16. 439 F. App'x 165 (3d Cir. 2011).
17. *Id.* at 167.
18. *Id.*
19. *Id.*
20. *Id.* at 168.
21. *Id.* (citing Sandoz Pharms. Corp. v. Richardson-Vicks, Inc., 902 F.2d 222, 228–29 (3d Cir. 1990)).
22. *Id.*
23. *Id.* at 168–69.
24. 825 F. Supp. 2d 706 (E.D.N.C. 2011).
25. *Id.* at 708.

seismic anchors, were used by telecommunications companies, developed a "personal relationship with employees of Hilti . . . [and] recommended in internet postings that '[Boykin] anchors should not be used because of performance questions.' "[26] The court acknowledged that Boykin anchors have no performance questions and that Wong's reputation and false statements caused distributors to stop carrying Boykin anchors.[27] Nevertheless, the court granted the defendant's motion to dismiss because Wong's postings were not commercial speech, AT&T did not compete commercially with Boykin, and there was no indication that the postings "were designed to influence consumers to buy products or services provided by Wong or AT&T Services, as opposed to Hilti."[28]

NTP Marble, Inc. v. AAA Hellenic Marble, Inc. offers a contrast. There, NTP Marble (also known as Colonial) filed a false advertising complaint against John Does after discovering numerous negative reviews about its services.[29] When responses to subpoenas revealed that several reviews came from "computers having IP addresses belonging to Hellenic's business office and/or the residence of one of its alleged directors," Colonial filed an amended complaint, naming Hellenic.[30] An Hellenic employee, Moser, who had previously worked for Colonial and also had a criminal background, then drafted a "statement" taking sole responsibility for posting the reviews, and Hellenic argued that it was therefore entitled to summary judgment.[31] Concluding that Colonial had produced evidence "from which a reasonable jury might conclude that Moser did not post all of the Reviews, and/or that he did so with the knowledge or encouragement" of Hellenic, the court denied summary judgment.[32] The court found that a jury could find the reviews constituted false advertising because they "were disseminated over the internet, and warned potential customers of Colonial's purported poor quality goods and workmanship, [and] suggested that customers take their business elsewhere."[33] The court held that the Lanham Act did not require that the reviews name Hellenic because a "violation may be found where the speech is commercial, refers to a specific product or service, and is motivated by economic interests."[34]

Courts have also found false advertising related to cybersquatting. In *Trafficschool.com, Inc. v. Edriver, Inc.*,[35] the plaintiffs marketed traffic school and driver's education courses, competing for referrals with the defendants, who owned and managed DMV.org, a website that helped people renew driver's licenses, buy car insurance, view driving records, beat traffic tickets, register

26. *Id.*
27. *Id.*
28. *Id.* at 711.
29. NTP Marble, Inc. v. AAA Hellenic Marble, Inc., 2012 U.S. Dist. LEXIS 24671, at *3 (E.D. Pa. Feb. 24, 2012).
30. *Id.* at *4–5.
31. *Id.* at *5–6.
32. *Id.* at *17–18.
33. *Id.* at *26.
34. *Id.*
35. 653 F.3d 820, 824 (9th Cir. 2011).

vehicles, and find DUI/DWI attorneys. The plaintiffs claimed that the defendants engaged in false advertising "by actively fostering the belief that DMV.org is an official state DMV website, or is affiliated or endorsed by a state DMV."[36] The court found that the website likely misled consumers because anyone in California who googled "dmv" or "drivers ed" would see sponsored listings for "ca.dmv.org" or "California.dmv.org" with links resolving to DMV.org.[37] That site also used state slogans and symbols and linked to web pages that helped consumers complete DMV-related transactions.[38] The court found that DMV.org's disclaimed connection with state DMVs was insufficient because it was "in small font at the bottom of each page, where many consumers would never scroll."[39] DMV.org used similar online marketing strategies in other states, and the plaintiffs showed actual confusion, which caused consumers to share sensitive personal information.[40] The court issued an injunction and awarded attorney's fees.[41]

In *Skydive Arizona, Inc. v. Quattrocchi*,[42] Skydive Arizona, a very large skydiving center, sued SKYRIDE, an internet and telephone-based skydive booking service, for false advertising, trademark infringement, and cybersquatting. Although Skydive Arizona did not accept bookings via SKYRIDE, some of SKYRIDE's numerous websites specifically referred to Arizona, and its registered domain names included skydivearizona.net, arizonaskydive.com, and skydivingarizona.com.[43] The district court granted Skydive Arizona's request for partial summary judgment on its false advertising claim, and a jury found in its favor on the other claims.[44] SKYRIDE disputed the district court's materiality finding, but the appellate court affirmed the lower court, finding Skydive Arizona's "decision to proffer declaration testimony instead of consumer surveys to prove materiality [did] not undermine its motion for partial summary judgment."[45] While the appellate court reversed the lower court's actual damages enhancement, it upheld the other damages of more than $5 million.[46]

II. Consumer Class Action Suits

The past year has also seen several class action complaints for false advertising. Hall of Famer George Brett's company, which sold ionic necklaces, reached a settlement with an Iowa man, who had filed a class action complaint for false advertising, alleging that Brett Bros. falsely claimed its products provided a number

36. *Id.*
37. *Id.* at 827.
38. *Id.* at 827–28.
39. *Id.* at 828.
40. *Id.*
41. *Id.* at 829–34.
42. 673 F.3d 1105, 1108 (9th Cir. 2012).
43. *Id.* at 1109.
44. *Id.*
45. *Id.* at 1111.
46. *Id.* at 1114–15.

of health benefits.[47] Still pending are suits in Florida and California against General Mills related to the company's claims on the internet (and other media) about the digestive health benefits of its YoPlus yogurt.[48] In *Fitzpatrick v. General Mills, Inc.*, the district court granted class certification and, after the Eleventh Circuit—on interlocutory appeal—remanded the case for further consideration, redefined the class to include "all persons who purchased Yo-Plus in the State of Florida until the date notice is first provided to the class."[49] In *Johnson v. General Mills, Inc.*, the district court reconsidered its grant of class certification after the U.S. Supreme Court issued a decision in a separate case that clarified the requirements for a finding of commonality under Rule 23(a) and after the *Fitzpatrick* court redefined the class.[50] The district court concluded that it was appropriate to include fourth generation purchasers in the class, noting, among other points, that the defendant "continued to present an explicit assertion that YoPlus improved digestive health on its website."[51] It will be important to follow the evolution of these cases, along with other recently filed class action suits for false advertising on the internet.[52]

III. Federal Trade Commission Actions

The Federal Trade Commission ("FTC") has the dual role of protecting consumers and promoting competition.[53] It "polices the internet for deceptive ads, and recently brought a slew of cases involving questionable advertising techniques."[54] Given the FTC's statutory authority,[55] the agency can bring actions for deceptive marketing practices where private actions, including class actions, were unsuccessful. In a case involving negative-option marketing, the FTC successfully obtained a settlement when private plaintiffs could not obtain personal jurisdiction over the defendants.[56] The FTC filed a broader case against the defendants for multiple online deceptive activities related to selling health and beauty supplements, operation of penny auctions, and a very broad research service.[57] The FTC claimed the online purchasers were not adequately informed

47. Thompson v. Brett Bros. Sports Int'l, Inc., No. 12-cv-0055-JAJ, slip op. at 1 (S.D. Iowa May 15, 2012) (order).

48. Fitzpatrick v. General Mills, Inc., 2011 U.S. Dist. LEXIS 138939 (S.D. Fla. Dec. 2, 2011); Johnson v. General Mills, Inc., 278 F.R.D. 548 (C.D. Cal. 2012).

49 *Fitzpatrick*, 2011 U.S. Dist. LEXIS 138939, at *4. The Eleventh Circuit's decision is *Fitzpatrick v. General Mills, Inc.*, 635 F.3d 1279, 1283 (11th Cir. 2011).

50. *Johnson*, 278 F.R.D. at 550 (citing Wal-Mart Stores, Inc. v. Dukes, 131 S. Ct. 2541 (2011)).

51. *Id.* at 551.

52. *See, e.g.*, De Keczer v. Tetley USA, Inc., No. 12-cv-02409-HRL (N.D. Cal. filed May 11, 2012); *In re* Match.com, No. 10-cv-02651-L (N.D. Tex. filed Nov. 16, 2011).

53. Fed. Trade Comm'n, Federal Trade Commission Annual Report 2012, at ii (Mar. 2012), *available at* http://www.ftc.gov/os/highlights/2012/ftc-highlights.pdf.

54. *Id.* at 9.

55. Federal Trade Commission Act §§ 4, 5, 12, 13, 15 U.S.C. § 44, 45, 52, 53 (2006).

56. *See* Fasugbe v. Willms, 2011 U.S. Dist. LEXIS 56569 (E.D. Cal. May 26, 2011) (court granted motion to dismiss plaintiffs' first amended complaint for failure to allege personal jurisdiction); Fasugbe v. Willms, 2011 U.S. Dist. LEXIS 93483 (E.D. Cal. Aug. 22, 2011) (court granted motion to dismiss plaintiffs' second amended complaint on the same ground).

57. FTC v. Willms, 2011 U.S. Dist. LEXIS 103160, at *3 (W.D. Wash. Sept. 13, 2011).

that the service was not "free" and that they were being enrolled in a recurring fee program unless they opted out shortly after placing an order.[58] After the FTC obtained an injunction, the defendants agreed to a settlement order, including an injunction banning them from using "negative-option" marketing and a judgment of $359 million, which was suspended upon the defendants meeting certain obligations.[59]

The FTC successfully pursued two groups of internet marketers of açai berry supplements. The first group of defendants, using negative-option marketing, offered a "free" sample, but the sample was free only if the customer returned the unused portion of the sample within fourteen days after having obtained company authorization.[60] The defendants did not disclose to consumers that, by signing up for a free sample, they also signed up for monthly shipments of the product unless they cancelled the plan.[61] Under an agreed order, the defendants were banned from selling any product with a negative-option feature and paid $1.5 million to the FTC.[62] The second group of defendants marketed açai berry products using fake internet news sites, such as nbssnewsat6.com, channel9investigates.com, channel2local.com, and channel9heathbeat.com, which featured fake news reports touting the benefits of açaiberry products.[63] The defendants agreed to a permanent injunction and a payment of $1.345 million.[64]

Another FTC action targeted a party that used paid search results on Google's search engine and Google ads on third-party websites to attract consumers who were in debt.[65] The company claimed it could reduce a consumer's debt by 70 percent but failed to disclose that its own fee was up to 30 percent of any savings and that the consumer's debt would continue to increase while it paid money to the defendant.[66] The company agreed to a final judgment of $3.3 million and an injunction preventing it from making such representations in the future.[67]

Mobile apps were also targeted by the FTC. The apps "AcneApp" and "Acne Pwner" claimed to treat acne with colored lights emitted from smartphones or

58. *Id.* at *4.

59. Stipulated Final Judgment and Order at 9–11, 18–24, FTC v. Willms, No. 11-cv-828-MJP (E.D. Wash. Feb. 22, 2012), *available at* http://www.ftc.gov/os/caselist/1023012/120223jwillmsstip.pdf.

60. Complaint at 5–8, FTC v. Cent. Coast Nutraceuticals, Inc., No. 10-cv-4931 (N.D. Ill. Aug. 5, 2010), *available at* http://www.ftc.gov/os/caselist/1023028/100816centralcoastcmpt.pdf.

61. *Id.* at 8–9.

62. Stipulated Order at 8–16, 19–25, FTC v. Cent. Coast Nutraceuticals, Inc., No. 10-cv-4931 (N.D. Ill. Jan. 3, 2012), *available at* http://www.ftc.gov/os/caselist/1023028/120109centralcoaststip.pdf.

63. Amended Complaint at 3–6, FTC v. IMM Interactive, Inc., No. 11-cv-2484 (N.D. Ill. Mar. 14, 2012), *available at* http://www.ftc.gov/os/caselist/1023232/120321copeaccmpt.pdf.

64. Stipulated Final Judgment at 2, 8–19, FTC v. IMM Interactive, Inc., No. 11-cv-2484 (N.D. Ill. Mar. 15, 2012), *available at* http://www.ftc.gov/os/caselist/1023232/120321copeacstip.pdf.

65. Complaint at 3–4, 7, FTC v. FDN Solutions, LLC, No. 12-cv-00820-JST (C.D. Cal. May 25, 2012), *available at* http://www.ftc.gov/os/caselist/1123078/120606fdncmpt.pdf.

66. *Id.* at 3–7.

67. Stipulated Final Judgment and Order at 2, 5–12, FTC v. FDN Solutions, LLC, No. 12-cv-00820-JST (C.D. Cal. May 25, 2012), *available at* http://www.ftc.gov/os/caselist/1123078/120606fdnstip.pdf.

mobile devices.[68] There were about 3,300 downloads of Acne Pwner at 99 cents each and about 11,600 downloads of AcneApp at $1.99 each.[69] After the FTC charged that the claims for both apps were unsubstantiated, the defendants agreed to stop making claims that their apps could treat acne.[70]

IV. Conclusion

Cases involving alleged false advertising in cyberspace have increased significantly in number but with varying degrees of success. Courts have recently found in favor of companies complaining of false advertising when a competitor's website contains false or misleading statements. On the other hand, not all courts are willing to conclude that similar statements in blog posts or pseudonymous reviews constitute false advertising given concerns about the true identity of posters and a lack of clarity regarding the credence consumers give to such posts and reviews. Courts have found, however, that the use of misleading domain names can give rise to false advertising claims. Recent class action complaints by consumers alleging false advertising on company websites have yielded mixed results, but the FTC has been very successful in reaching settlements in both internet and mobile application cases. As the internet and social media continue to grow as favored vehicles for marketing, we are likely to see many more cases involving false advertising using these media with perhaps a clearer pattern of what it will take for a plaintiff to prevail.

68. *In re* Brown, FTC Docket No. C-4337 (Oct. 13, 2011) (decision and order); *In re* Finkel, FTC Docket No. C-4338 (Oct. 12, 2011) (decision and order).

69. *See supra* note 68.

70. *See supra* note 68.

Trademarks and Copyrights in Cyberspace: A Year in Review

*By Kristine F. Dorrain and Jonathan T. Rubens**

Introduction

This year's trademark and copyright survey is combined to highlight the increasing effect of cyberspace on intellectual property law. Keyword advertising online continues to be a hot topic, as does the definition of what is copyrightable. We revisit the first sale doctrine this year, further exploring developments in the law as affected by internet sales. Finally, we conclude each section with some trends: for trademark law we look into a couple of cases of aggressive enforcement, and for copyright law we look into the development of the law surrounding how content owners are attempting to find online infringers and what the various courts are permitting.

I. Trademark Law Developments

This year our trademark survey once again updates the case law involving use of trademarks as keywords, internet search characteristics, and trademark infringement online.[1] We also consider cases that raise questions about zealous trademark advocacy by luxury brands and others, leaving open the door to even more zealous advocacy in the future but with an uncertain cost.[2]

* Kristine Dorrain is Director of Internet and IP Services at Forthright, where she manages the National Arbitration Forum's arbitration and mediation programs, including its internationally recognized program for resolving trademark disputes online under the Uniform Domain Name Dispute Resolution Policy. In her spare time, she teaches Intellectual Property Appellate Practice at William Mitchell College of Law and coaches several IP-related moot courts. She is currently the Cyberspace Law Committee's Director of Programming and the editor of this survey. Jonathan Rubens is a cofounder of Javid Rubens LLP in San Francisco, where his practice focuses on commercial transactions, startups and emerging companies, and intellectual property protection. He regularly advises entrepreneurs and investors on new venture formation, represents businesses and investors in equity financings, mergers and acquisitions, and acts as outside general counsel advising businesses on a wide variety of commercial transactions and IP issues. Mr. Rubens is the chair of the American Bar Association's Cyberspace Law Committee. The authors wish to thank Rick Dold, Steven Kinsella, and Stephanie Morales, law clerks with Forthright, for their invaluable research and editing assistance.

1. *See infra* Part I.A.
2. *See infra* Part I.B.

A. Trademarks and the Internet

We focus on four cases this year that pick up where we left off discussing the impact of the internet on trademarks and advertising in the survey last year.[3] Google's Ad Words program was back in front of the U.S. Court of Appeals in *Rosetta Stone Ltd. v. Google, Inc.*, where the Fourth Circuit echoed the Ninth Circuit in finding that all of the circuit's infringement factors should be considered to see if they fit the facts of an infringement claim, but that not every factor would be relevant in every case.[4] Interestingly, the discussion did not turn on the much-debated definition of "use in commerce," as the court noted the parties seemed to have agreed that it was.[5] The court took the analysis a step further, however, in deciding that Google's "sale" of Rosetta Stone's mark as a keyword for its sponsored links program was "referential or nominative in nature" and that made rote application of all of the factors particularly unsuitable.[6]

Google had recently updated its policies, in 2009, to allow the purchase of trademarks as keywords in limited situations, which was a change from its 2004 policy (where Google had noted such allowance would cause confusion).[7] Rosetta Stone argued that the change drastically increased the number of sites selling counterfeit products, that its customers were being misled, and that Google, based on its 2004 analysis, knew that the change would cause confusion.[8] The court found that Google's 2004 admission, that allowing the purchase of keywords could cause confusion, raised a genuine issue of fact as to the intent of Google to infringe.[9] Regarding actual confusion, the Fourth Circuit noted that, while the three types of evidence proffered by Rosetta Stone were not overwhelming, Rosetta Stone did demonstrate evidence of actual confusion.[10]

Finding that Rosetta Stone had provided just enough doubt on its factual contentions to overcome summary judgment on the three "disputed" likelihood of confusion factors, the court addressed Google's argument that its use of the Rosetta Stone marks as keywords was protected by the functionality doctrine.[11] The court distinguished Google's use of Rosetta Stone's marks from Rosetta Stone's use of its own marks and found that the applicable test was whether Rosetta Stone's use of its marks was functional, and the court found it was not.[12]

3. Kristine F. Dorrain, *The Cyberspace Survey of Recent Trademark Cases*, 67 Bus. Law. 349, 350 (2011) (discussing Network Automation, Inc. v. Advanced Sys. Concepts, Inc., 638 F.3d 1137 (9th Cir. 2011), with the Ninth Circuit clarifying that no infringement factor is most determinative but all factors should be considered in each likelihood of confusion analysis).

4. 676 F.3d 144, 155 (4th Cir. 2012).

5. *Id.* at 152–53.

6. *Id.* at 154.

7. *Id.* at 151.

8. *Id.* at 152.

9. *Id.* at 155–56.

10. *See generally id.* at 156–60 (noting that Rosetta Stone presented evidence of unwitting purchases of counterfeit products, which caused doubt as to the level of consumer sophistication).

11. *Id.* at 161. The functionality doctrine says that a trademark or trade dress is not protectable if it is a functional feature that would limit competition if protected. *Id.* (citing Qualitex Co. v. Jacobson Prods. Co., 514 U.S. 159, 164–65 (1995)).

12. *Id.* at 162.

The lower court pointed to *Tiffany (NJ) Inc. v. eBay Inc.* in finding that Rosetta Stone had not provided sufficient notice of infringement.[13] Rosetta Stone had supplied Google with a spreadsheet of advertisers using sponsored links to sell counterfeit merchandise and, though Google removed the ads for the websites listed, Google allowed those same sponsors to purchase Rosetta Stone's keywords for different sites.[14] This created a sufficient question of fact to survive summary judgment as to contributory liability, despite *Tiffany*, in which the court had made a determination of "generalized" notice after trial.[15]

As to vicarious liability, the court quickly affirmed summary judgment in Google's favor, finding no evidence that Google had acted jointly with any advertisers.[16] Similarly, the court concluded that "Rosetta Stone failed to allege facts showing that it 'conferred a benefit' on Google for which Google 'should have reasonably have expected' to repay," and found nothing to prevent affirmation of Google's motion to dismiss on Rosetta Stone's claims of unjust enrichment.[17]

On dilution, the lower court had granted summary judgment for Google on two bases: first, Rosetta Stone did not present evidence that Google was using Rosetta Stone's marks to "identify its *own* goods and services." On this point the court remanded for the lower court to first determine if Rosetta Stone had made a prima facie case for dilution as set forth in the Fourth Circuit's *Louis Vuitton* case and then to determine whether Google had been able to demonstrate its use was fair.[18] Second, Rosetta Stone did not provide evidence that "Google's use of the mark was likely to impair the distinctiveness of or harm the reputation of the ROSETTA STONE marks."[19] This second basis for the lower court's finding was also in error because the court emphasized actual injury to Rosetta Stone, when the question was whether Google's use was *likely* to impair the distinctiveness of the marks.[20] The Fourth Circuit concluded its opinion with direction to the lower court to determine 1) when Google first began to dilute Rosetta Stone's marks (if at all) and then 2) whether Rosetta Stone's marks were famous at the time the dilution began.[21]

The U.S. District Court for the Northern District of California was not as reluctant to grant summary judgment in *Groupion, LLC v. Groupon, Inc.*, where it granted defendant Groupon's motion for summary judgment, despite the similarity of the marks.[22] Several infringement factors were found in Groupon's favor: while the names "Groupon" and "Groupion" are spelled similarly, the

13. *Id.* at 163–64 (discussing the lower court's reliance on *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir. 2010)).
14. *Id.* at 163.
15. *Id.* at 165.
16. *Id.*
17. *Id.* at 166.
18. *Id.* at 170 (citing Louis Vuitton Malletier S.A. v. Haute Diggity Dog, LLC, 507 F.3d 252, 264–65 (4th Cir. 2007)).
19. *Id.* at 168.
20. *Id.* at 171.
21. *Id.* at 172–73.
22. No. 11-00870, 2012 WL 1655728, at *2 (N.D. Cal. May 8, 2012) (stressing that Groupion's arguments were unsupported by admissible evidence in the record).

court found the two marks were not pronounced the same, did not have the same look in the marketplace, and were coined with different meanings.[23] The two companies are largely unrelated in that Groupon offers a "deal of the day" coupon service and Groupion provides custom software solutions featuring integrated environments.[24] The court found that the area of overlap between Groupon's enhancements and Groupion's primary software business was not sufficient to tip the factor in Groupion's favor because a "reasonable finder of fact could not find that a business which needs comprehensive customer management software would turn to Groupon because they may obtain some information about their customers who purchase Groupons or because Groupon now offers an online calendar service."[25]

The primary significance of this case for practitioners may be the discussion of the trademark infringement factor "shared marketing channels."[26] The court applied *Network Automation* and *Playboy*, both discussed in last year's survey, to start with the premise that the use of the internet to market one's goods and services is so ubiquitous, that, without more, the mere fact of online sales is meaningless.[27] The court found no shared marketing channels, as Groupon did not market its product in or toward business software environments.[28] The quite brief consideration of the similarity of the marks, the relatedness of the goods and services, and the overlap of the marketing channels indicates that the courts are giving consumers, or maybe internet search engines, a lot of credit, or responsibility, for distinguishing between the goods and services of various brand owners.

Keywords and YouTube tags as trademark use-in-commerce were considered in *Naked Cowboy v. CBS*,[29] in which the New York City street performer, recognized as "nearly naked" by briefs, cowboy hat, boots, and guitar, brought suit against a CBS soap opera for an episode in which a character, dressed up in briefs, cowboy hat, and boots, sang and played the guitar.[30] The words "Naked Cowboy" were not spoken or written anywhere during the episode.[31] Following the airing of the episode, however, it was posted to CBS's YouTube channel with the title "The Bold and the Beautiful—Naked Cowboy" and to the "boldandbeautiful" YouTube channel, which used the tags "naked" and "cowboy."[32] Finally, the defendants purchased the words "naked" and "cowboy" as keywords from

23. *Id.* at *3.
24. *Id.* at *4–5 (listing scheduling coupon usage, allowing business to reward frequent users, and providing business with some customer data as the only potential overlapping enhancements).
25. *Id.* at *6.
26. *Id.* (discussing the Ninth Circuit's trademark infringement test, as set forth in *AMF Inc. v. Sleekcraft Boats*, 599 F.2d 341 (9th Cir. 1979)).
27. *Id.* (discussing Network Automation, Inc. v. Advanced Sys. Concepts, Inc., 638 F.3d 1137, 1151 (9th Cir. 2011); Playboy Enters., Inc. v. Netscape Commc'ns Corp., 354 F.3d 1020, 1028 (9th Cir. 2004)); Dorrain, *supra* note 3, at 350.
28. *Groupion*, 2012 WL 1655728, at *6.
29. 844 F. Supp. 2d 510 (S.D.N.Y. 2012).
30. *Id.* at 512–13.
31. *Id.* at 513.
32. *Id.* at 513–14.

YouTube, such that searches for "Naked Cowboy" would result in high-ranking "hits" for the defendants' video.[33] We consider the court's trademark analysis of the keyword purchases, online advertising, and video title.

First, it is not entirely clear what logic the court applied to find that the tags used on YouTube were not a use in commerce, except that it seems to be significant that the tags were for "naked" and "cowboy" and not for "naked cowboy."[34] Second, the court found that the keyword advertising and purchase of the specific term "naked cowboy" was not a use in commerce because the terms were not placed on goods or containers (ostensibly for sale) and the words were not used to indicate source.[35] Further, the court found that the words "Naked Cowboy" were only used as the *descriptive* title of the clip, which was therefore a fair use.[36] At that point, the court fully ended its analysis of the keywords and tags and dismissed the plaintiff's trademark infringement claim.[37] The rather cursory dismissal of the keyword and YouTube tag uses of the mark are puzzling given that CBS was using the trademarked term to promote (a.k.a. "sell") its soap opera. The court seemed to focus on the fact that the real distinction of The Naked Cowboy's marks was tied up in the specifics of the entertainer's trade dress (the dollar signs on the boots and the words "Naked Cowboy" on his briefs, guitar, and hat) and seemed to believe that absent those elements, the term and remaining trade dress were not protectable.[38] And the court seems to assume consumers are generally unlikely to be confused simply because of a video title and tags. Whether or not plaintiff would have succeeded, it appears that the facts alleged should have survived the motion to dismiss and we are not surprised to see a Notice of Appeal was filed on March 23, 2012.

Internet searches involving another's mark and the similarity of marketing channels also were significant factors in a California federal court's denial of toymaker Hasbro's motion for a preliminary injunction against Asus Computer International for Asus's new tablet computers.[39] Hasbro sells toy "transforming" robots called Transformers, which have become a series of comic books, television shows, and motion pictures.[40] The "good guys" are led by a robot named Optimus Prime.[41] Asus makes and sells computer processors, including tablet com-

33. *Id.* at 514.
34. *Id.* at 515.
35. *Id.* The court took 15 U.S.C. § 1127 literally, it seems, noting that "The Naked Cowboy" was not used on goods or documents relating to the goods. *Id.*
36. *Id.*
37. *Id.* at 516.
38. *Id.* at 512–13 (describing the costume); *id.* at 516–17 (outlining the elements the court found to be distinctive). The court's discussion of the trade dress, to which the *Polaroid* factors are applied, did not consider the combination of the word mark and trade dress, either, and the court found the trade dress of the actor in the soap opera to be "not similar" to the "distinctive" elements of The Naked Cowboy. *Id.* at 517 (citing Polaroid Corp. v. Polaroid Elecs. Corp., 287 F.2d 492, 495 (2d Cir. 1961)).
39. Hasbro, Inc. v. Asus Computer Int'l, Inc., No. 11-10437 (C.D. Cal. 2012), *available at* http://www.scribd.com/doc/99060362/Hasbro-Inc-v-Asus-Computer-International-Inc.
40. *Id.* at 1–3.
41. *Id.*

puters that "transform" from a tablet to a laptop computer with the addition of peripheral hardware, called Eee Pad Transformer TF 101,[42] and it recently launched a premium or "Prime" option.[43] Hasbro contended the Asus tablets infringed its marks in "Transformers" and "Prime," particularly since Transformers had sought and received product placement and other advertising/co-branding with electronics giant LG and with computer peripheral manufacturers (for after-market skins).[44]

The court's consideration of the *Sleekcraft* factors, specifically the court's handling of the "marketing channels and degree of care used by consumers" factors, is of particular interest because Hasbro focused heavily on internet search results and internet sales in its contentions.[45] As a result, the court directed its attention to *Network Automation* yet again.[46]

The court reminded the parties that search results on the internet are easily distinguished by the reasonable consumer and that it is unreasonable to rely on Google or Amazon searches because the purpose of those sites is to aggregate data.[47] The court reasoned that users searching for "transformer" or "transformers" are faced with many choices besides those of the parties and are quickly confronted with the source and other information relating to the products retrieved.[48] The court further reasoned that, because Asus's product was a high-end item, consumers were likely to exercise a greater degree of caution in purchasing.[49] The remaining *Sleekcraft* factors balanced in favor of Asus and the court declined to award the preliminary injunction.[50]

These cases confirm the significance of the *Network Automation* case and emphasize the shift that courts are experiencing in discussing the impact of the internet, search engines, keywords, and e-commerce on the determination of trademark use and infringement.

B. Zealous Trademark Advocacy: The Ex Parte Process and Vexatious Litigation

Our final trademark-related cases share a common characteristic: both have elements of the extreme in the verdicts. First, in an ex parte process, designer Hermès was permitted to obtain a temporary restraining order and preliminary injunction against thirty-four domain names that included a variation of

42. *Id.* at 3–4.
43. *Id.* at 4. The "Prime" tablet featured the newest Google operating system, added a metallic spun casing, and was a "premium device." *Id.*
44. *Id.* at 2.
45. *Id.* at 6–7 (detailing the factors for infringement from *AMF, Inc. v. Sleekcraft Boats*, 599 F.2d 341, 348–49 (9th Cir. 2003)); *see also id.* at 13–15 (analyzing the "marketing channels" factor).
46. *Id.* (citing Network Automation, Inc. v. Advanced Sys. Concepts, Inc., 638 F.3d 1137, 1150 (9th Cir. 2011)).
47. *Id.* at 14–15.
48. *Id.* at 15.
49. *Id.* Interestingly, the court did not address whether Hasbro's customers would be confused. *Id.*
50. *Id.* at 15–18.

Hermès's mark and sold at least nine types of counterfeit goods.[51] The defendants defaulted and, forty-three days after the case was filed, the court awarded statutory damages of 100 million dollars.[52] Plaintiffs also received seizure of defendants' PayPal accounts; entitlement to Defendants' property; a permanent injunction against future infringement, false advertising, and spoliation of evidence regarding infringement; and an injunction preventing defendants from setting up new infringing organizations.[53] Not only the domain name registry but also other third-party providers, such as registrars, ISPs, payment processing services, and shippers, are required to withhold services from defendants in conjunction with the infringing domain names.[54]

Of the litany of punishments meted out against defendants, the most "extreme" were, of course, the statutory damages award but also the breadth of the injunction. It would appear Hermès can pretty much wave the order at anyone with the power to make a change affecting the domain names and force it to comply. The inclusion of payment processors, search engines, and shippers as parties to enforce the order, as well as the ability to come back and add more domain names to the list later,[55] with the court's permission, make the scope of the injunction, in a default case where defendants were served via electronic mail, appear extremely aggressive.

Our final "extreme" case is one involving litigious 1-800-Contacts.[56] 1-800-Contacts had sued Lens.com for trademark infringement, breach of contract, and a bevy of other related claims for purchasing keywords and internet advertisements that 1-800-Contacts believed violated its marks, and the court granted summary judgment to Lens.com.[57] Now seeking attorney's fees and costs Lens.com complained of 1-800-Contacts' litigation strategy of trying to drive smaller competitors out of business and of employing improper litigation tactics to drive up the costs of litigation.[58] The judge granted 1-800-Contacts some leeway in its aggression, noting that the main legal issue in the case involved an unsettled area of law given the emerging and changing nature of internet competition.[59] "The Tenth Circuit has never expressly addressed whether purchasing another's trademark as a keyword constitutes trademark infringement, and such cases have survived motions to dismiss in other jurisdictions."[60]

The court's view may be surprising as many may view fairly well settled the proposition that the keyword purchases alone did not constitute infringement.

51. Hermès Int'l v. John Doe 1, No. 12-cv-01623-DLC, slip op. at 1, 5–6 (S.D.N.Y. 2012), *available at* http://www.scribd.com/doc/92046940/Hermes-v-Does-12-Civ-1623-S-D-N-Y-Apr-30-2012-Judgment.
52. *Id.* at 6 (awarding statutory damages on the trademark claims, per 15 U.S.C. § 1117(c)(2)).
53. *Id.* at 7–9.
54. *Id.* at 9.
55. *Id.* at 10.
56. 1-800-Contacts, Inc. v. Lens.com, Inc., No. 7-cv-591 CW, 2012 WL 113812 (D. Utah Jan. 13, 2012).
57. *Id.* at *1.
58. *Id.* at *2.
59. *Id.* at *3.
60. *Id.*

Nevertheless, the court found both parties' conduct was not "fully candid."[61] The court commented that 1-800-Contacts' style was "aggressive" and its "actions raise questions about vexatious suits" but found that there was not enough in the record to find that 1-800-Contacts did more than was necessary to protect its rights and declined to award attorney's fees to Lens.com.[62]

Both the 1-800 Contacts case and the Hermès case may demonstrate judicial tolerance of "extreme" litigation strategies in cases involving internet business practices and online trademark assets, when those same tactics might not have been allowed in an offline context.

II. Copyright Law Developments

This year's survey of copyright law brings four new cases to the forefront, touching on issues of copyrightability and assignment, as well as further exploring the relationship between the copyright first sale doctrine and licensing agreements.[63] We conclude with some trends, including a case surveyed last year and changes in copyright litigation tactics.[64]

A. Protectability of "Structure, Sequence, and Organization"—*Oracle America, Inc. v. Google Inc.*

As technology and cyberspace continue to permeate our culture, so, too, does the definition of what is copyrightable. This year, technology giants Oracle and Google took to the courts in California for some resolution on whether the "structure, sequence, and organization of [Oracle's] Java application programming interface are protected by copyright."[65] In this case, Google had attempted to license use of Oracle's Java programming language and platform so that it could adapt it for mobile devices, but negotiations broke down.[66] As a result, Google decided to use the Java language to write its own code for its Android mobile devices, and, over time, Google was able to replicate the functionality of some of Java's APIs, as needed for its mobile device.[67] Because the attraction of Java is its cross-platform functionality, it was necessary for Google's engineers to make its program compatible with the way Java operates; as a result, though the code was different, it had to function the same way, so the code had to be arranged into "packages" consistent with the way the Java application would look for them.[68] Ultimately, the question before the court was "whether Google was and remains free to replicate the names, organization of those names, and

61. *Id.* at *4.
62. *Id.*
63. *See infra* Part II.A–C.
64. *See infra* Part II.D.
65. Oracle Am., Inc. v. Google Inc., No. 10-03561, 2012 WL 1964523, at *1 (N.D. Cal. May 31, 2012).
66. *Id.* at *3.
67. *Id.* The court provided a very thorough, lay-friendly discussion of how Java works, describing the folder and command structure very clearly. *Id.* at *3–8.
68. *Id.* at *2–3.

functionality of 37 out of 166 packages in the Java API, which has sometimes been referred to in this litigation as the 'structure, sequence, and organization' of the 37 packages."[69]

The court analyzed cases from many other circuits, noting that, while the specific issue before the court had never been addressed in any other circuit, other courts had found copyrightability in "structure, sequence, and organization."[70] The court focused on the facts of this case, noting that Google had been careful not to copy the copy itself, that the file structure was required for functionality, and that the file names were unprotectable as "titles."[71] Ultimately, the court decided the following:

> So long as the specific code used to implement a method is different, anyone is free under the Copyright Act to write his or her own code to carry out exactly the same function or specification of any methods used in the Java API. . . . When there is only one way to express an idea or function, then everyone is free to do so and no one can monopolize that expression.[72]

Other than being a significant victory for Google in the mobile phone wars, this case is fascinating in both the way the judge delved into the minutiae of how Java worked and in his chronicling of the history of the law. Judge Alsup also referenced the trend of companies to apply for software patents in increasing numbers, while seeking less copyright protection.[73] He noted the observations of a commentator:

> As software patents gain increasingly broad protection, whatever reasons there once were for broad copyright protection of computer programs disappear. Much of what has been considered the copyrightable "structure, sequence and organization" of a computer program will become a mere incident to the patentable idea of the program or of one of its potentially patentable subroutines.[74]

The court challenges the notion (as seen in Part I) that intellectual property protection is sacred and deserves unquestioning and absolute protection. This idea that not everything someone can come up with or devise is protectable is the equivalent to heresy in some circles. The battle between patent and copyright protection for software will only heat up in the next year or so, as companies are forced to choose, then live with, the legal ramifications of their choice.

B. The First Sale Doctrine

Two significant cases this year addressed issues involving the limitation on copyright known as the first sale doctrine. A recent case involving another

69. *Id.* at *4.
70. *See generally id.* at *13–23; *see also id.* at *23 (noting the "trajectory in which enthusiasm for protection of 'structure, sequence, and organization' peaked in the 1980s").
71. *Id.* at *25–26, *28.
72. *Id.* at *2.
73. *Id.* at *23.
74. *Id.* (quoting Mark Lemley, *Convergence in the Law of Software Copyright?*, 10 High Tech. L.J. 1, 26–27 (1995)).

technology giant, Apple,[75] discussed allegations related to first sale and copyright misuse and revisited a case we discussed last year, *Vernor v. Autodesk, Inc.*[76] Apple, a computer hardware and software manufacturer, sued Psystar, a computer hardware manufacturer, for copying Apple's Mac OS X operating system into Psystar's "Open Computers."[77] When Psystar manufactured its computers, it used purchased copies of Apple's Mac OS X software, which it loaded onto a Mac computer it owned.[78] It then "unlocked" and slightly modified the software to override the encryption that only allowed the software to work on Apple computers and imaged it to the Psystar computer.[79] An original, unopened Apple Mac OS X copy was included with each purchase.[80] Apple contended that its software was licensed, not sold, to purchasers of its Mac computers and that 1) the purpose of the software was for existing Apple users to upgrade their operating system and 2) the license agreement limited the software's use to Apple computers.[81] Psystar counterclaimed for a declaratory judgment stating that, subject to the first sale doctrine, its purchase of the Mac OS X software exhausted Apple's copyright protection and that the suit was simply a matter of Apple trying to retain control it did not have, as copyright misuse.[82]

Relying heavily on its holding in *Vernor*, the Ninth Circuit determined that software licenses are "ubiquitous" and have "become the preferred form of software transactions" but then noted that copyright misuse has been the rallying cry of licensees that wish to limit the scope of the licenses.[83] The court noted that copyright misuse can amount to "'egregious' anticompetitive restraint" and that the purpose of the defense is to prevent copyright owners from overextending their limited monopoly.[84] Similar to the court in *Oracle America, Inc. v. Google Inc.*, the court here found that the real issue was whether the restriction unreasonably restricted the development of competing products.[85] Ultimately, the court held, as Apple urged, that Apple's license did not.[86] The Ninth Circuit affirmed the permanent injunction against Psystar.[87]

The Second Circuit also addressed first sale, this time in the context of international sales and agreements.[88] John Wiley & Sons manufactures academic books and textbooks for sale worldwide, using a wholly owned subsidiary for

75. Apple Inc. v. Psystar Corp., 658 F.3d 1150 (9th Cir. 2011).

76. *See* Dorrain, *supra* note 3, at 327 (discussing Vernor v. Autodesk, Inc., 621 F.3d 1102 (9th Cir. 2010)).

77. *Apple*, 658 F.3d at 1153. Open Computers can run a variety of operating systems. *Id.*

78. *Id.*

79. *Id.*

80. *Id.*

81. *Id.*

82. *Id.* at 1154–55.

83. *Id.* at 1155–57. The court held that Apple's license did satisfy the three-factor *Vernor* test in distinguishing between a license and sale. *Id.* at 1159.

84. *Id.* at 1157.

85. *Compare* Oracle Am., Inc. v. Google Inc., No. 10-03561, 2012 WL 1964523, at *2 (N.D. Cal. May 31, 2012), *with Apple*, 658 F.3d at 1158–60.

86. *Apple*, 658 F.3d at 1160.

87. *Id.* at 1162.

88. John Wiley & Sons, Inc. v. Kirtsaeng, 654 F.3d 210 (2d Cir. 2011).

foreign sales.[89] All foreign-distributed books contain a printed restriction that they are for distribution only in the region specified.[90] Kirtsaeng was a university math student from Thailand who enlisted the help of family and friends to send him textbooks that were purchased in Asia for much less than the U.S. cost; Kirtsaeng then resold those books on eBay, reimbursed his suppliers and pocketed the profit, as a means of subsidizing his education.[91]

Wiley sued for copyright infringement and the court refused to allow Kirtsaeng to provide a first sale defense, claiming it did not apply to foreign-manufactured works.[92] The Second Circuit undertook the responsibility to parse the meaning of "lawfully made under this title" and to determine whether or not the textbooks were considered as such would be outcome-determinative on the first sale issue.[93] The court considered 17 U.S.C. § 602(a)(1), which prohibits importation of copyrighted works into the United States, and weighed the two statutory provisions.[94] In the end, the court determined that the best interpretation of § 109(a) is that it applies "only to copies manufactured domestically."[95] The dissent noted that the majority's holding provides "greater copyright protection to copies manufactured abroad than those manufactured domestically,"[96] a point that perhaps the majority was addressing when it pointed out that Congress is free to correct the situation if the court had erred in its holding.[97]

These two first sale cases demonstrate just how much the cyberworld has opened up new avenues for the exploitation of copyrighted works. The proliferation of online auction sites for selling merchandise acquired more cheaply elsewhere and the advent of entrepreneurs looking to use, improve upon, or incorporate the digital works of others blur the boundaries and will present courts with more interesting and novel fact patterns in coming years.

C. Copyright Assignment

We next touch briefly on another case where cyberspace plays a significant role in how a copyright ownership dispute was resolved.[98] Coca-Cola contracted with Universal Music Latin America to have a Spanish version adapted from the anthem it had recorded for the 2010 FIFA World Cup soccer tournament.[99]

89. *Id.* at 212–13.
90. *Id.* at 213.
91. *Id.*
92. *Id.* at 213–14.
93. *Id.* at 216; *see* 17 U.S.C. § 109(a) (2006) ("[T]he owner of a particular copy . . . lawfully made under this title . . . is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy.").
94. *John Wiley & Sons*, 654 F.3d at 216.
95. *Id.* at 220–21 (citing 17 U.S.C. § 109(a); *id.* § 602(a)(1); Quality King Distribs., Inc. v. L'anza Res. Int'l, Inc., 523 U.S. 135 (1998)).
96. *Id.* at 227–28.
97. *Id.* at 222.
98. Hermosilla v. Coca-Cola Co., 446 F. App'x 201 (11th Cir. 2011).
99. *Id.* at 201.

Universal Music Latin America teamed up with Universal Music Publishing Group to find and select Rafael Vergara Hermosilla ("Vergara") to adapt the song in November 2009.[100] It appears there was no written agreement at that time.[101] Vergara finished work in December 2009 and sent an invoice for $6,000, but when iTunes Mexico began selling the song in February 2010, Vergara was not credited with the adaptation.[102]

Vergara attempted to negotiate a settlement and sent an e-mail on March 4, 2010 stating that his "only demand" was credit as an adaptor and that the song should be considered work made for hire for the value of one dollar.[103] The same day, Universal Group assigned the copyright interests to Coca-Cola, and the assignment noted that the rights from Vergara had been assigned to Universal Group, which was then assigning them to Coca-Cola.[104] On March 5, Universal Group accepted the e-mailed offer, but on March 8, Vergara notified it that the deal was just a proposal and that Vergara was revoking it.[105] The district court eventually granted summary judgment to Coca-Cola on the basis of the e-mailed offer and acceptance.[106]

What is most interesting about this case is that it was not until the work was already being sold that there was any mention of the work being a work made for hire.[107] To be a work made for hire, the statute requires there to be a writing, signed by both parties.[108] Here, the court permits a few e-mails to suffice, perhaps because of the inclusion of the magic words "work for hire," but never addresses the timing of the writing.[109]

D. The Latest Developments in Copyright Law

Last year, we surveyed *Golan v. Holder*, a case by a group of musicians challenging the constitutionality of section 514 of the Uruguay Round Agreements Act ("URAA") based on the effect the URAA had of removing some works from the public domain.[110] This year, the Supreme Court determined that the additional copyright protection granted to the public domain works was still limited in time and that the alignment of the United States with other Berne Convention nations was an appropriate exercise of congressional power.[111]

100. *Id.* at 201–02.
101. *Id.* at 202.
102. *Id.*
103. *Id.*
104. *Id.*
105. *Id.* at 203.
106. *Id.* The Eleventh Circuit affirmed summary judgment due to the e-mail communication. *Id.*
107. *Id.* at 202–03 (making no mention of another contract and treating Vergara's e-mail and the parties' conversations as evidence of the essential terms of the contract).
108. 17 U.S.C. § 101 (2006).
109. *See* 1 Melville B. Nimmer & David Nimmer, Nimmer on Copyright § 5.03 (2000) (discussing when the work for hire writing should take place and noting that some circuits do permit a later writing to document the parties' intent).
110. *See* Dorrain, *supra* note 3, at 339 (discussing Golan v. Holder, 609 F.3d 1076 (10th Cir. 2010), *cert. granted*, 79 U.S.L.W. 3271 (U.S. Mar. 7, 2011) (No. 10-545)).
111. Golan v. Holder, 132 S. Ct. 873, 885, 894 (2012).

The Court shot down the idea that removing works from the public domain was an impingement on free speech, finding that, since Congress had the power to protect the works initially, nothing prohibited Congress from correcting the mistake that let the works slip into the public domain prematurely.[112]

Our final development for this year comes in a brief overview of a series of cases dealing with the identification of John Doe respondents charged with illegally downloading copyrighted content. Several circuits are grappling with the litigation tactics of a handful of firms that have set themselves up in the business of handling these cases.[113] Notably, all of these cases involve the file-sharing network BitTorrent, which works by creating a "swarm" of users looking to download a particular work.[114] The file is downloaded piecemeal until all users have received all the necessary bits of the work, which are then reassembled into the whole work on the user's computer.[115] Plaintiffs in these cases have filed suit against the infringers, knowing only their Internet Protocol ("IP") addresses; they are moving for the courts to issue subpoenas against the Internet Service Providers ("ISPs") to obtain the customer contact information associated with the IP addresses.[116] In several cases, some of the John Doe Defendants moved to quash the subpoenas or otherwise protested.[117]

In *Call of the Wild*, the court spent a great deal of time determining that the plaintiff was deserving of the subpoena based on judicial and financial economy.[118] It also found that the way BitTorrent worked was enough to satisfy the requirement that the infringement stemmed from the "same transaction or occurrence" and that "a file sharer's First Amendment right to anonymity is exceedingly small."[119] The California magistrate judge in *Hard Drive Productions* found joinder improper because it would present a great hardship to all defendants to have to receive and deal with all of other defendants' pleadings.[120] Additionally, the court found that the infringement was not necessarily part of the same transaction or occurrence, so dismissing the complaint as to all but one defendant was proper.[121] The Massachusetts judge in *Liberty Media* did permit joinder and found that the infringement was part of the same transaction.[122]

112. *Id.* at 892.

113. *See* Call of the Wild Movie, LLC v. Does 1–1,062, 770 F. Supp. 2d 332 (D.D.C. 2011); Hard Drive Prods., Inc. v. Does 1–188, 809 F. Supp. 2d 1150 (N.D. Cal. 2011); Liberty Media Holdings, LLC v. Swarm Sharing Hash File, 821 F. Supp. 2d 444 (D. Mass. 2011); K-Beech, Inc. v. Does 1–57, No. 11-cv-358-FtM-36SPC, 2011 WL 5597303 (M.D. Fla. Nov. 1, 2011); *In re* BitTorrent Adult Film Copyright Infringement Cases, No. 11-3995, 2012 WL 1570765 (E.D.N.Y. May 1, 2012) (citing additional similar cases).

114. *See, e.g.*, *Call of the Wild*, 770 F. Supp. 2d at 339.

115. *Id.*; *see also Liberty Media*, 821 F. Supp. 2d at 448.

116. *See, e.g.*, *BitTorrent*, 2012 WL 1570765, at *1.

117. *See, e.g.*, *Liberty Media*, 821 F. Supp. 2d at 446–47; *see also K-Beech*, 2011 WL 5597303, at *1.

118. 770 F. Supp. 2d at 344.

119. *Id.* at 343, 349.

120. Hard Drive Prods., Inc. v. Does 1–188, 809 F. Supp. 2d 1150, 1164 (N.D. Cal. 2011) (noting the resources the court would also expend on such litigation).

121. *Id.* at 1165.

122. *Liberty Media*, 821 F. Supp. 2d at 452–53.

The judge in *Liberty Media* was the first to note defendants' speculation that "Liberty Media sought the public identities of Does 1–38 to coerce pretrial settlement," but found that to be too speculative to affect his decision.[123] However, the judge then also ruled that defendants, faced with a trial for possibly downloading hardcore homosexual pornography, could not proceed anonymously.[124] A magistrate judge from Florida was persuaded by the *Call of the Wild* case to permit joinder and deny the motions to quash based on judicial economy in *K-Beech*; she noted that the joinder could actually be beneficial to defendants, who would benefit from seeing other defenses.[125] Finally, another New York magistrate judge, who noted that "[t]hese actions are part of a nationwide blizzard of civil actions" brought against BitTorrent users, recommended dismissal of all four consolidated cases before it, except as to the first defendant in two of the cases.[126] The court was persuaded by testimony as to plaintiff K-Beech's coercive negotiation tactics, even when faced with evidence of defendant's innocence.[127] The judge also found joinder improper because the infringement did not necessarily arise from the same transaction or occurrence, but also because the various possible defenses of defendants were so unique that it would actually waste judicial resources to juggle it all.[128] Finally, the judge noted that the whole point of these lawsuits was for the copyright holder to gain a lot of data while paying only one filing fee, which the court found was improper based on the statutory requirement to maintain the court system by paying fees.[129]

These cases are ongoing and we have only touched on a few representative examples for illustrative purposes. As more and more courts deal with these cases and hear testimony about the litigation tactics alleged, it is possible courts will be able to arrive at a consensus in the year to come in dealing with these types of cases.

Conclusion

Clearly, the internet plays a significant role in the way brand and content owners are managing, and forced to police, their intellectual property. We expect to see a continued shift in the protection of software from primarily copyright protection to an increased use of patent protection. We anticipate that keywords will remain a hot topic next year, and look forward to watching the development of the BitTorrent litigation strategies as well.

123. *Id.*
124. *Id.*
125. K-Beech, Inc. v. Does 1–57, No. 11-cv-358-FtM-36SPC, 2011 WL 5597303, at *2, *4, *6 (M.D. Fla. Nov. 1, 2011).
126. *BitTorrent*, 2012 WL 1570765, at *1.
127. *Id.* at *5. "[O]btaining the home telephone numbers seems calculated to further plaintiff's settlement strategies . . . rather than advancing their claims by allowing them to effect service." *Id.* at *8.
128. *Id.* at *11–12.
129. *Id.* at *13.

Survey of Domain Name Cases 2011–2012

*By Leland Gardner**

As in last year's survey,[1] several of this year's Anticybersquatting Consumer Protection Act ("ACPA")[2] cases analyze the definition of a "bad faith intent to profit."[3] Another case examines a domain name registrar's potential liability under the ACPA for domain forwarding.[4] And a Ninth Circuit decision considers whether re-registration of a domain name can support a cyberpiracy claim.[5]

A survey of Uniform Domain Name Dispute Resolution Policy ("UDRP")[6] cases illustrates how individuals can prevent others from unauthorized use of their personal names.[7]

I. Cases Brought Under the Anticybersquatting Consumer Protection Act

A. Bad Faith Intent to Profit

A threshold question in ACPA cases is whether the alleged cybersquatter had a "bad faith intent to profit" from the disputed domain name.[8] Section 1125 of the ACPA provides nine factors to guide courts in making this determination—but how long the defendant owned the domain name is not among them according to the court in *Travelers Indemnity Co. v. Travellers.com*.[9]

The plaintiff brought an in rem action against TRAVELLERS.COM alleging several violations of the Lanham Act and cybersquatting.[10] The plaintiff moved for summary judgment, and the registrant of the disputed domain

* Leland Gardner is an intellectual property attorney with Fish & Richardson, P.C.

1. *See* Leland Gardner, *Domain Name Cases 2010–2011*, 67 Bus. Law. 361, 364–65 (2011).
2. 15 U.S.C. § 1125(d) (2006).
3. Bogoni v. Gomez, No. 11-cv-08093, 2012 WL 745548 (S.D.N.Y. Jan. 6, 2012); Am. Univ. of Antigua Coll. of Med. v. Woodward, No. 10-cv-10978, 2011 WL 6187429 (E.D. Mich. Dec. 5, 2011); Travelers Indem. Co. v. Travellers.com, No. 10-cv-448, 2011 WL 5975082 (E.D. Va. Nov. 28, 2011).
4. Petroliam Nasional Berhad v. GoDaddy.com, Inc., No. 09-cv-5939, 2012 WL 10532 (N.D. Cal. Jan. 3, 2012).
5. GoPets Ltd. v. Hise, 657 F.3d 1024 (9th Cir. 2011).
6. *Uniform Domain Name Dispute Resolution Policy*, Internet Corp. for Assigned Names & Numbers (Aug. 26, 1999), http://www.icann.org/en/dndr/udrp/policy.htm.
7. *See infra* notes 52–57 and accompanying text.
8. *See Travelers Indem. Co.*, 2011 WL 5975082, at *7.
9. *Id.*
10. *Id.* at *1.

name, Mr. Deepak Rajani of Germany, filed a belated opposition.[11] In his opposition, Mr. Rajani argued primarily that he had "a first-come, first-served right to the domain name" based on his twelve years of using TRAVELLERS.COM.[12]

The court disagreed.[13] Relying upon the nine statutory factors, the court stated that Mr. Rajani's long-time use was "immaterial to the question of bad faith under the ACPA," and ultimately found that seven of the nine factors weighed in favor of finding bad faith.[14] The court therefore granted the plaintiff's motion for summary judgment.[15]

Courts often find the nine-factor analysis useful in determining whether bad faith exists. Indeed, the court in *Bogoni v. Gomez* imported this analysis into a seldom-litigated provision of the ACPA—section 8131—which prohibits the unauthorized registration of a person's name with a "specific intent to profit."[16]

The defendant created a website at PAULBOGONI.ORG that included, among other things, an offer to sell the domain name for $1 million.[17] The plaintiff, Paul Bogoni, filed a complaint and requested a preliminary injunction, contending that the defendant's actions violated section 8131 of the ACPA.[18] Noting that there was "very little case law interpreting section 8131, and less concerning the statutory term 'specific intent to profit,' " the court reasoned that the nine factors of section 1125 would be helpful in conducting its analysis and found that the factors weighed in favor of the plaintiff.[19] Furthermore, the court found that the defendant's offer to sell the domain name for far more than its value to anyone other than the plaintiff was "strongly probative of a specific intent to profit."[20] The court determined that the plaintiff was likely to succeed on the merits, and granted the plaintiff's motion for a preliminary injunction.[21]

The nine statutory bad faith factors, however, are neither exclusive nor mandatory under section 1125 as demonstrated in *American University of Antigua College of Medicine v. Woodward*.[22] The defendant, Mr. Steven Woodward, was a former medical student at American University of Antigua College of Medicine who was discharged without receiving a degree.[23] Mr. Woodward subsequently established a website at AUA-MED.COM to complain about various alleged bad acts and misrepresentations by the Antiguan medical school.[24]

11. *Id.*
12. *Id.* at *7.
13. *Id.*
14. *Id.*
15. *Id.* at *8.
16. Bogoni v. Gomez, No. 11-cv-08093, 2012 WL 745548, at *3 (S.D.N.Y. Jan. 6, 2012).
17. *Id.* at *1.
18. *Id.* at *2.
19. *Id.* at *3–4.
20. *Id.* at *5.
21. *Id.* at *6.
22. Am. Univ. of Antigua Coll. of Med. v. Woodward, No. 10-cv-10978, 2011 WL 6187429, at *6 (E.D. Mich. Dec. 5, 2011).
23. *Id.* at *1.
24. *Id.*

The medical school filed a complaint against Mr. Woodward asserting defamation, various Lanham Act violations, and cybersquatting.[25] In determining whether Mr. Woodward had a bad faith intent to profit, the court recited the nine statutory factors, but then stated that it "must evaluate the relevance of these factors in light of the statute's intended purpose."[26] The court went on to consider a similar case in which the defendant created a website solely to criticize the plaintiff.[27] Specifically, in *Lucas Nursery & Landscaping v. Grosse*, the Sixth Circuit held that, even though most of the factors weighed against the defendant, its conduct was not the type proscribed by the ACPA.[28] The court found *Lucas Nursery* persuasive, concluding that "registering a website with a domain name identical to or confusingly similar to the plaintiff's for the sole purpose of 'cyber-griping' is not the type of activity made illegal by the ACPA."[29]

B. Domain Name Registrar Liability for Domain Forwarding

Merely forwarding domain name traffic to existing websites does not violate the ACPA, according to the court in *Petroliam Nasional Berhad v. GoDaddy.com, Inc.*[30] Among other functions, domain name registrars like GoDaddy perform domain name resolution—the process of converting between domain names, which are meaningful to humans, and IP addresses, which are used by internet infrastructure for routing traffic.[31] Essentially, domain name resolution involves configuring a nameserver so that requests for a given domain name are routed to the desired website.[32] Registrars offer several configuration options when a registrant purchases a domain name.[33] For example, the nameserver can be configured to point to a default "coming soon" page or to a new website hosted by the registrar or another party.[34] Registrars will even configure the nameserver so that traffic is forwarded to an existing website with a preexisting domain name.[35] This final configuration is referred to as "domain name forwarding."[36]

The plaintiff Petroliam Nasional Berhad, known as "Petronas," is the Malaysian national oil company.[37] In its lawsuit, Petronas claimed that GoDaddy was liable for cybersquatting and contributory cybersquatting because it forwarded traffic for the PETRONASTOWER.NET and PETRONASTOWERS.NET

25. *Id.* at *1.
26. *Id.* at *5–6.
27. *Id.* at *6.
28. 359 F.3d 806, 809–11 (6th Cir. 2004).
29. *Am. Univ. of Antigua Coll. of Med.*, 2011 WL 6187429, at *7.
30. Petroliam Nasional Berhad v. GoDaddy.com, Inc., No. 09-cv-5939, 2012 WL 10532, at *9 (N.D. Cal. Jan. 3, 2012).
31. *Id.* at *2.
32. *Id.*
33. *Id.*
34. *Id.*
35. *Id.*
36. *Id.* at *3.
37. *Id.*

domain names to various pornographic websites.[38] GoDaddy sought summary judgment on the cybersquatting claim, arguing that it did not "use" the domain name as required by the ACPA, and further that it had no bad faith intent to profit from the Petronas trademark.[39] GoDaddy also contended that it could not be liable for contributory cybersquatting because: (a) contributory cybersquatting is not a cognizable claim; (b) Petronas failed to prove bad faith intent on the part of the actual domain name registrant; and (c) GoDaddy did not directly control or monitor the actual registrant.[40]

The court agreed that GoDaddy was not liable for cybersquatting because domain name forwarding "does not amount to 'use' of the domain names."[41] The court also noted that because GoDaddy did not charge for domain name forwarding, it lacked the requisite intent to profit.[42] While the court also agreed that GoDaddy was not liable for contributory cybersquatting, it disregarded GoDaddy's first argument—that contributory cybersquatting is not a viable claim.[43] As in *Microsoft Corp. v. Shah* from last year's survey,[44] the *Petroliam Nasional* court assumed that contributory cybersquatting could be a valid claim.[45] However, because Petronas provided no proof on the underlying cybersquatting claim, and because merely providing "an Internet routing service" cannot constitute "direct control and monitoring" of cybersquatting, the court found that there was no contributory cybersquatting.[46]

C. Re-Registration of a Domain Name Is Not "Registration" Under the Act

The ACPA does not prohibit a registrant from re-registering (i.e., transferring to another entity) a domain name that is confusingly similar to another's mark, according to the Ninth Circuit in *GoPets Ltd. v. Hise*.[47] In *GoPets*, a Ninth Circuit panel reviewed a grant of summary judgment in favor of GoPets on its ACPA and Lanham Act claims.[48] A key issue on appeal was whether re-registration constitutes a "registration" as defined in the ACPA.[49]

Relying on the ACPA's text and traditional property law, the Ninth Circuit held that only the initial registration was a "registration."[50] The panel explicitly disagreed with an opposite Third Circuit holding in *Schmidheiny v. Weber*

38. *Id.* at *1.
39. *Id.* at *5–6.
40. *Id.* at *9.
41. *Id.*
42. *Id.*
43. *Id.* at *10.
44. No. C10-0653, 2011 WL 108954 (W.D. Wash. Jan. 12, 2011).
45. 2012 WL 10532, at *10.
46. *Id.* at *12.
47. 657 F.3d 1024, 1032 (9th Cir. 2011).
48. *Id.* at 1029.
49. *Id.* at 1026.
50. *Id.* at 1030–32.

because it would "make rights to many domain names effectively inalienable," a result that Congress could not have intended.[51]

II. Cases Brought Under the Uniform Domain Name Dispute Resolution Policy

The UDRP, like section 8131 of the ACPA, allows individuals to stop unauthorized use of their personal names by third parties, even though the names may not be registered trademarks.[52] Unfortunately for the complainants in *Fagin v. Cox*, *Mashberg v. Cox*, and *Leccese v. Cox*, a trio of rulings by an administrative panel at the WIPO Arbitration and Mediation Center, the UDRP requires a threshold showing that the personal name has become "a distinctive identifier associated with the complainant or its goods or services."[53] Each of these cases involved a "well-known and highly []respected attorney" of the Proskauer Rose, LLP law firm, whose personal name was allegedly misappropriated by the same respondent, Crystal Cox.[54] In ruling against complainants, the panel explained that there was no evidence that the attorneys' names were commercially recognized apart from their firm.[55]

In contrast, another panel found that complainant Nicole Richie, a "well-known actor and spokesperson" was entitled to common law rights in her personal name.[56] Accordingly, the panel ordered that the NICOLERICHIEFRANCE.COM and NICOLERICHIEPERFUME.COM domain names be transferred from the registrant to Ms. Richie.[57]

III. Conclusion

The ACPA and UDRP cases surveyed this year probed the ever-shifting boundaries of these laws, and we hope that next year will bring additional clarity. The surveyed cases also illustrate how dynamically these laws can be applied to complicated factual situations.

51. *Id.* at 1031–32 (analyzing Schmidheiny v. Weber, 319 F.3d 581, 583 (3d Cir. 2003)).

52. *See* Mouret v. Domains by Proxy, Inc., No. D2009-1435, at *3–4 (WIPO Dec. 10, 2009).

53. Fagin v. Cox, No. D2011-0678, 2011 UDRP LEXIS 1319 (WIPO June 30, 2011); Mashberg v. Cox, No. D2011-0677, 2011 UDRP LEXIS 1346 (WIPO June 30, 2011); Leccese v. Cox, No. D2011-0679, 2011 UDRP LEXIS 1320 (WIPO June 30, 2011).

54. *Fagin*, 2011 UDRP LEXIS 1319, at *3–5; *Mashberg*, 2011 UDRP LEXIS 1346, at *2–5; *Leccese*, 2011 UDRP LEXIS 1320, at *2–5.

55. *Fagin*, 2011 UDRP LEXIS 1319, at *8–9; *Mashberg*, 2011 UDRP LEXIS 1346, at *8–9; *Leccese*, 2011 UDRP LEXIS 1320, at *8–9.

56. Richie v. Ahuja, No. D2012-0500, 2012 UDRP LEXIS 1030, at *2–3 (WIPO Apr. 19, 2012).

57. *Id.* at *14.