Survey of the Law of Cyberspace: Introduction

*By Jonathan T. Rubens and Edward A. Morse**

Surveyors play an important role in exploring the unknown. Nearly 300 years ago, Lord Fairfax appointed seventeen-year-old George Washington to the post of surveyor.[1] His measurements would become instrumental for future progress in settling a wilderness. Measuring, recording, and mapping provide a means for us to comprehend space, so that we can order it and use it. This process starts by identifying the major landmarks, and then filling in details to create a more comprehensive map of the landscape.

Our surveyors have been mapping the terrain of cyberspace law for almost twenty years, and there has been much to explore this year. The landmarks in this space are becoming more familiar—including privacy, data security, and challenges of regulating new technologies—and the map for making this space habitable for business, consumers, and government is developing granularity.

Our first surveyor, Roland Trope, provides a broad perspective on cybersecurity practices.[2] Drawing from three developments coming from different legal sources—an Executive Order, a First Circuit decision, and an FTC enforcement action—Trope sees a pivotal turn toward enhancing the responsibility of businesses for proactive behavior to protect their customers from cybersecurity threats.[3] When the specter of cyber-threats affects one's own commercial well-being, the incentives for protection are evident. However, incentives are not always so clear when it comes to a responsibility to protect the interests of others, such as customers or third parties, from threats delivered through a business's

* Jonathan Rubens is the chair of the Cyberspace Law Committee and is co-founder of Javid | Rubens LLP in San Francisco, where his practice includes commercial transactions, emerging companies, business acquisitions, and intellectual property. Edward A. Morse is the editor of this year's annual Survey of the Law of Cyberspace. He is a professor at Creighton University School of Law in Omaha, Nebraska, where he holds the McGrath, North, Mullin & Kratz endowed Chair in Business Law. His scholarship includes exploration of the intersection between legal standards, private ordering, and technology in matters of privacy and data security. The authors acknowledge the contributions of Creighton University law students Clark Youngman and Maxwell Crawford, who worked faithfully, diligently, and competently to complete important work for this survey.

1. See Harrison Clark, 1 All Cloudless Glory: The Life of George Washington 25 (1998).

2. Roland L. Trope, *Bearings from the Southern Cross: Cybersecurity Decisions 2012–2013*, 69 Bus. Law. 189 (2013).

3. *See id.* at 197.

software or infrastructure. Trope suggests this is changing, and that this is a cause for initiating new conversations with business clients.[4]

Civil liability threats create an important incentive structure affecting the emerging responsibilities for security in cyberspace. John Black provides new details about the legal environment for data security breach liability.[5] As Black shows, despite growing attention to the need for security, breaches continue to occur and they continue to be expensive.[6] That expense primarily consists of remediation and notification costs, as well as in the economic consequences from damaged customer relationships. At the same time, mass liability claims from affected customers continue to face formidable challenges in the areas of standing, class certification, and proof of damages.

Legislative intervention intended to clarify the parameters of liability threats in cyberspace and to create safe harbors in which new generations of businesses might flourish online has not always been well-received or fully understood. The parameters for immunity under 47 U.S.C. § 230, which protects users and providers of an "interactive computer service" from liability for certain online content, have frequently become the subject of judicial interpretation. Catherine Gellis covers these developments, as well as those involving copyright claims under the DMCA (17 U.S.C. § 512).[7]

Cyberspace differs from other uncharted territories in that it already contains so many remnants of human occupation. Our personal information is everywhere; what are we to do with it? Does our privacy still matter, and if so, can we do anything to protect it? It has become quite clear that lawless hackers are hardly the only threat to our privacy, as business and government have both taken an interest in collecting and using personal data, which can be done quickly, inexpensively, and invisibly, using a variety of technologies.

Four articles in this year's survey address the matter of privacy, reflecting the breadth and importance of these issues in understanding the landscape of cyberspace. First, John Pavolotsky takes on the topic of "big data," which he describes counterintuitively as becoming increasingly a matter of "small data."[8] Although some privacy issues have been raised in the criminal law context (including GPS tracking), Pavolotsky focuses primarily on the commercial environment, where behavior has primarily been shaped by contract. He also lays out some sensible options for risk mitigation that firms with data should consider.

Second, Fatima Kahn delves into the matter of FTC privacy enforcement actions with a detailed tour of several major enforcement actions against business firms.[9] Some of these cases involve regulated areas, such as credit reporting,

4. *See id.* at 190.

5. John Black, *Developments in Data Security Breach Liability*, 69 BUS. LAW. 199 (2013).

6. *Id.* at 199–200.

7. Catherine R. Gellis, *2013 State of the Law Regarding Intermediary Liability for User-Generated Content*, 69 BUS. LAW. 209 (2013).

8. John Pavolotsky, *Privacy in the Age of Big Data*, 69 BUS. LAW. 217 (2013).

9. Fatima N. Kahn, *Survey of Recent FTC Privacy Enforcement Actions and Developments*, 69 BUS. LAW. 227 (2013).

where laws such as the FCRA and GLB Act require attention to privacy and data collection practices. But others may reflect an agency attempt to define appropriate security practices without specific statutory guidance. In one of these actions (*In re Wyndham Worldwide*),[10] the targeted business is pushing back and challenging the FTC's authority to act in setting data security standards. The FTC has been an important contributor to the development of privacy protections for consumers, relying primarily on its authority to address unfair competition. This litigation raises an important question about the FTC's institutional powers, which merits watching.

Robert Hale contributes further to the privacy discussion through his article addressing the particular environment of mobile privacy.[11] The mobile environment presents special challenges for a model based on private ordering, as consumer notification and consent limitations are particularly acute in an environment of small screens that is targeted to the consumer in constant motion. The FTC has played an important role here, too, not only through enforcement actions but also through releasing a new business guide addressing the need for mobile application developers to develop reasonable data security. As Hale also points out, state privacy laws are also in play here, potentially subjecting businesses to competing sovereign demands in our own federal system.[12] As mobile devices become the primary means to access the internet, tradeoffs between utility and privacy are likely to receive further attention from regulators and consumer advocates.

In the fourth article in our privacy segment, Katherine Ritchey, Mauricio Paez, Veronica McGregor, and Maria Sendra address competing sovereign demands in connection with global privacy and data security topics.[13] Ritchey and her colleagues address problems with jurisdictional and substantive legal issues associated with the cloud, including competing regulatory regimes of the United States and European Union. While also touching on mobile privacy, their article provides some comparative analysis of global privacy and data security considerations in the European Union and beyond, along with some predictions about likely directions for new developments.

Moving back to the domestic front, electronically stored information (ESI) has become a perennial topic for litigators dealing with the reality of modern record-keeping and discovery practices. Timothy Chorvat and Laura Pelanek again address this important topic.[14] Their discussion of predictive coding reminds us that lawyers need to innovate to survive.[15] They also discuss cases implementing

10. Complaint, FTC v. Wyndham Worldwide Corp., No. 12CV01365, 2012 WL 2389423 (D. Ariz. June 26, 2012), *available at* http://www.ftc.gov/os/caselist/1023142/120626wyndamhotelscmpt.pdf.

11. Robert V. Hale, II, *Recent Developments in Mobile Privacy Law and Regulation*, 69 Bus. Law. 237 (2013).

12. *Id.* at 237.

13. Katherine Ritchey et al., *Global Privacy and Data Security Developments*, 69 Bus. Law. 245 (2013).

14. Timothy J. Chorvat & Laura E. Pelanek, *Electronically Stored Information in Litigation*, 69 Bus. Law. 255 (2013).

15. *See id.* at 255–260.

the proportionality principle in discovery planning, which seeks to address the economic realities of litigation and their relationship to ethical obligations.[16]

This year Stephen Middlebrook joins Sarah Jane Hughes to tackle the increasingly significant topic of electronic payments and financial services.[17] This year saw more developments in new payment mechanisms, including virtual currencies like Bitcoin that have garnered significant media attention. As virtual currencies have overcome traditional market-based problems associated with inducing consumer participation, regulators and law enforcement officials have taken notice. Concerns about money laundering, crime, and global terrorism have induced the Departments of Justice and Homeland Security, as well as FinCEN, to take actions that show an intention to police the virtual currency market aggressively.[18] As Middlebrook and Hughes also point out, more traditional payment mechanisms have also generated legal developments this year, and we continued to see state and federal regulators expand their reach to address not only the payment system but also the matter of unused funds.[19] As a relative newcomer to this regulatory party, the CFPB has been making new rules affecting prepaid cards, which include effects on the operation of state escheat laws.[20]

Cyberspace is a fertile environment for intellectual property issues. The near-frictionless environment for the dissemination of ideas and images offers immense potential for human flourishing, but it also presents enforcement challenges for owners of property rights. Jonathan Rubens addresses developments affecting copyrights in cyberspace.[21] After covering the major copyright development from the Supreme Court—its opinion in *Kirtsaeng* expanding the first use defense to infringement[22]—Rubens addresses other cases considering various ways that copyrighted content is reposted and redistributed online. This year, as before, technology innovators continued to push the boundaries of how information is distributed in a digital world, and the legal ramifications are not always clear. Meanwhile, copyright litigation marches on with more activity from the circles of aggressive copyright litigants and harsh judicial reactions.

In a separate article, Phong Nguyen explores recent developments in the Federal Circuit concerning patent infringement, including the knotty problem presented by what some have called "trolls" (known in more polite circles as "non-practicing entities").[23] As Nguyen also explains, the Obama Administration has recently identified the problems of litigation generated by non-practicing entities as a matter of concern.[24]

16. *See id.* at 260–62.
17. Stephen T. Middlebrook & Sarah Jane Hughes, *Virtual Uncertainty: Developments in the Law of Electronic Payments and Financial Services*, 69 BUS. LAW. 263 (2013).
18. *See id.* at 273.
19. *See id.* at 270–72.
20. *Id.*
21. Jonathan T. Rubens, *Copyrights in Cyberspace—Resales, Reposts, Rebukes*, 69 BUS. LAW. 275 (2013).
22. Kirtsaeng v. John Wiley & Sons, Inc., 133 S. Ct. 1351 (2013).
23. Phong D. Nguyen, *The Changing Scope of Patent Rights*, 69 BUS. LAW. 281 (2013).
24. *See id.* at 289.

Kenneth Caldwell provides an update on the fast-moving topic of internet gambling.[25] In December 2011, the U.S. Department of Justice issued a surprising opinion that effectively permitted some types of internet gambling that are not otherwise prohibited by state law.[26] This opinion reversed a longstanding interpretation of the Wire Act and otherwise restrictive law enforcement policies of the federal government, which have not been friendly to internet gambling operations.[27] Caldwell's article explores these new state laws and the implications of this new federal policy to the specter of expanded gambling operations in cyberspace.

Finally, we end this year's survey with a report from Renato Opice Blum and Rita P. Ferreira Blum, who provide an overview of developments in Brazil.[28] As cyberspace is becoming increasingly important to consumers and businesses in Latin America, this article explores developments in consumer protection law and criminal proscriptions affecting individuals and businesses operating in cyberspace. Like the United States, Brazil lacks a comprehensive legislative approach to addressing privacy and data security. Courts have thus emerged as an important venue for developing laws to facilitate consumer protection in this environment.

Our surveyors have thus compiled important and useful information and analysis, and we hope you will find enlightenment and profit in reading them. These authors have expended substantial time and effort, reflecting a strong professional commitment for which we are grateful.

25. Kenneth N. Caldwell, *The Shifting Tide in Internet Gambling—Survey of Recent Developments*, 69 Bus. Law. 291 (2013).

26. Whether Proposals by Illinois and New York to Use the Internet and Out-of-State Transaction Processors to Sell Lottery Tickets to In-State Adults Violate the Wire Act, 35 Op. O.L.C. 1 (Sept. 20, 2011), *available at* http://www.justice.gov/olc/2011/state-lotteries-opinion.pdf.

27. Caldwell, *supra* note 25, at 292–93.

28. Renato Opice Blum & Rita P. Ferreira Blum, *Recent Developments in Cyberspace Law: A View from Brazil*, 69 Bus. Law. 301 (2013).

Bearings from the Southern Cross: Cybersecurity Decisions 2012–2013

*By Roland L. Trope**

I. Introduction

Imagine you have been aloft on the International Space Station throughout the year under review, April 2012–April 2013. On your return to your earthbound office your colleagues ask, "*What was it like up there—to see continents and oceans in a glance? What was it like to see the big picture without details and distractions?*" After you answer, you might ask in reply, "*What did I miss that I should know about?*" Anticipating your question, your colleagues prepared this survey, which narrates three decisions that brought significant changes to the cybersecurity legal landscape. They signal a pivotal turn toward imposing enhanced responsibility for cybersecurity on businesses in the best position to improve it. In many cases, these businesses previously found ways to shift cybersecurity risks from themselves to their customers. The constellation of decisions in this survey should be illuminating to lawyers and clients and give them reasons to re-examine security- and incident-response procedures.

Section II of this survey reviews a First Circuit decision on U.C.C. Article 4A that reduces the ability of banks to shift online banking losses to customers. The decision does this by ultimately conditioning the validity of bank-customer agreements on whether the bank implemented and adhered to "commercially reasonable" security procedures. Section III analyzes a salient feature of the February 2013 Executive Order on cybersecurity for critical infrastructure—the Order's directions for sharing federal cyber intelligence with private companies. Private sector recipients of federal cyber intelligence may find that the intelligence comes with implicit responsibilities—to make good and expeditious use of it or risk being judged on the lack of preparedness they could have otherwise achieved. Section IV reviews a Federal Trade Commission ("FTC") action that targets deficiencies in a mobile device maker's software design process that undermined the integrity of its Android operating system's security. The complaint and resulting settlement represent a novel use of FTC enforcement power to

* Roland Trope is a partner in the New York City 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. The views expressed herein are his own and should not be attributed to the U.S. Military Academy, the Department of Defense, or the U.S. Government. The author thanks Professor Sarah Jane Hughes for her insightful editorial contributions to this survey.

sanction the software maker for failing to detect and remove security vulnerabilities during product design and development.

Each of these decisions responded to specific cyber threats by requiring companies to fulfill newly articulated, potentially expansive, corporate cyber-responsibilities. As you read, weigh these decisions and the changes in responsibilities that they illuminate. Consider them analogous to a constellation's stars in the night skies, light-years apart and yet the terrestrial viewer finds they illuminate a pattern. In this instance, it is of the constellation *Crux* (or *Southern Cross*)[1]: a navigational aid for mariners in the southern hemisphere as first sight of it "at sea is, to natives of the southern hemisphere, the sign that they are homeward bound."[2] For lawyers this constellation of decisions may aid them in navigating circumstances where there is no other warning of the ease with which security can abruptly "go south." To grasp the significance or *crux* of these decisions, readers will want to scrutinize their salient details and subtle nuances and to observe dark holes in the star field—where the decisions left crucial matter nebulous and unexplained.

II. How Bank Security Procedures May Fail to Be "Commercially Reasonable" Under U.C.C. Article 4A

Cybersecurity procedures alone do not assure safe online banking. When security protocols generate alerts, bank and payment processing personnel must review them and respond, taking into account "circumstances of the customer" known to the bank.[3] Failing to take these steps may render security procedures "commercially unreasonable" under U.C.C. Article 4A and deprive an originator's bank of the risk allocations and liability limits it sought in its online banking agreement with its customer.[4] That is the sea-change reading given to Article 4A in *Patco Construction Co., Inc. v. People's United Bank*.[5] The court's fact-intensive opinion demonstrates that the *crux* of security procedures will be the use—serious or superficial—a bank, or any business, makes of them. Although the outcome parallels the 2011 decision *Experi-Metal, Inc. v. Comerica Bank*,[6] *Patco* represents the first decision by a circuit court of appeals to impose such a high duty on banks. Other circuit courts may find it persuasive.

In 2003, Patco entered into written agreements with its bank governing Patco's use of electronic banking ("eBanking").[7] These agreements covered Patco's use of the ACH system for payroll purposes and certain funds transfers from

1. Five main stars make up the kite-shaped *Crux* or *Southern Cross*, which points almost directly south, unlike its dimmer, diamond-shape, neighboring constellation *False Cross*. *See* H.A. Rey, The Stars: A New Way to See Them 62–63 (1980).

2. The Oxford Companion to Ships & the Sea 818 (Peter Kemp ed. 1976).

3. *See* U.C.C. § 4A-202 (2011).

4. *Id.*

5. 684 F.3d 197 (1st Cir. 2013).

6. No. 09-14890, 2011 WL 2433383 (E.D. Mich. June 13, 2011). For analysis, see Roland L. Trope, *"There's No App for That": Calibrating Cybersecurity Safeguards and Disclosure*, 68 Bus. Law. 183 (2012).

7. *Patco*, 684 F.3d at 200.

one Patco account to another at the same bank or to an account at another bank.[8] They allocated almost all the risk of using eBanking and of any resulting loss to Patco, the customer.[9] The agreements limited the bank's liability to "gross negligence" and capped the amount of liability at six months of fees.[10] The agreements also provided that use of a customer's password qualified as "authentication of all transactions performed" by or on its behalf.[11]

The bank adopted and implemented a third-party vendor's security system that included key features such as: (1) *user authentication*—by entry of a company ID and password and a user-specific ID and password; (2) *device authentication*—by downloading a cookie into an eBanking customer's computers; (3) *risk profiling*—by generating a risk score (from 0 to 1,000) at each log-in attempt, derived from indicia such as IP address, device cookie ID, geo-location, and transaction activity; (4) *posing of challenge questions to authenticate the user* when a payment order's risk score surpassed 750 and blocking access if the user failed three times to give the correct answers; and (5) *a heightened risk check in the form of additional "challenge questions"* whenever a payment order exceeded a dollar amount set by the bank.[12] The bank did not monitor the risk profile reports that its security system generated.[13] Its personnel did not manually review payment orders that generated high risk scores or exceeded the risk-score threshold.[14] It did not call customers in the event of an atypical payment order. It also set the payment order risk check amount at $1,[15] which resulted in every transaction being subject to the heightened risk-check challenge question procedure.

On May 7, 2009, cyber-thieves used a Patco employee's ID and password credentials and answers to the challenge questions to initiate an ACH payment order of $56,594 from Patco's accounts.[16] The payment order departed significantly from Patco's previous eBanking activity.[17] The cyber-thieves directed payment to accounts of individuals who had never received funds from Patco.[18] The thieves logged in from an IP address Patco had never used. The bank's system computed a risk-score of 790—exceeding Patco's highest previous risk score of 214. The system also generated a report that attributed the 790 score to: "(1) 'Very high risk non-authenticated device'; (2) 'High risk transaction amount'; (3) 'IP anomaly'; and (4) 'Risk score distributor per cookie age.'"[19]

8. *Id.*
9. *Id.*
10. *Id.*
11. *Id.*
12. *Id.* at 203–04.
13. *Id.* at 212.
14. *Id.* at 204–05.
15. *Id.* at 203. The court does not explain why the bank took this action, or how Patco learned of the bank's superficial use of its security procedure. There are many gaps in the court's factual account.
16. *Id.*
17. *Id.* at 204.
18. *Id.*
19. *Id.* at 204–05.

How did the bank respond to these security flags? It did not. No one at the bank monitored high-risk transactions, and no one manually reviewed the May 7, 2009 order, despite the flags. The bank just processed it, sending $56,594 from Patco's account to unauthorized accounts. Building on their first success, the cyber-thieves repeated the ruse several times over the next few days, causing more than $400,000 to be sent from Patco's account.[20] For each transaction, the bank's system reported higher than usual risk scores. Each time, no bank personnel reviewed the reports or manually reviewed the transactions.[21] Moreover, the bank did not notify Patco of the transactions.[22]

The fraud came to the bank's attention because the thieves erred. They provided invalid account numbers for some of the transferees of the initial payment order.[23] The errors caused those transfers to fail.[24] Still unaware of the illicit activity, the bank sent "return notices" to Patco—not quickly by e-mail or fax, but by snail mail.[25] Patco received the first notice on the evening of May 13, a week after the initial unauthorized transaction.[26] Patco alerted the bank the next morning that this payment order was unauthorized.[27] Nonetheless, the bank processed a sixth unauthorized payment order for $111,693 that same morning.[28] The bank eventually blocked and recovered a portion of those funds.[29] By that time, the cyber-thieves had fraudulently withdrawn $588,851.26 from Patco's account.[30] Following some recovery efforts by the bank, Patco was left with a loss of $345,444.43.[31]

Patco sued the bank to recover the funds, but it faced a formidable obstacle in the eBanking agreements Patco had signed that purportedly made it liable for such losses.[32] So Patco attacked the enforceability of those agreements. It argued that, under Article 4A of Maine's Uniform Commercial Code ("Article 4A"), an agreement to limit a bank's liability for unauthorized, electronic funds transfers cannot be enforced if the bank failed to safeguard those services with commercially reasonable security procedures.[33]

On cross motions for summary judgment, the district court adopted the magistrate judge's findings that: (1) provisions of Article 4A displaced all other counts in Patco's complaint; and (2) the Article 4A count failed, because the bank's security procedures had been "commercially reasonable."[34] For those

20. *Id.* at 205.
21. *Id.* at 204–05.
22. *Id.* at 205.
23. *Id.*
24. *Id.*
25. *Id.*
26. *Id.*
27. *Id.*
28. *Id.*
29. *Id.*
30. *Id.*
31. *Id.*
32. *Id.* at 206.
33. *Id.*
34. *Id.*

reasons, the court agreed with the magistrate's recommendation and granted summary judgment for the bank.[35]

On Patco's appeal, the First Circuit reversed and remanded.[36] The First Circuit's opinion explained that Article 4A ordinarily allocates the risk of loss to a bank when it receives a payment order that results in an unauthorized funds transfer.[37] Article 4A permits a bank to shift that risk to its customer if the bank-customer agreement meets Article 4A's conditions: (1) bank and customer must have agreed that authenticity of the customer's payment orders would be verified by a security procedure; (2) the bank's security procedure must qualify as a "commercially reasonable method of providing security against unauthorized payment orders"; and (3) the bank must prove it "accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer."[38]

With good faith not at issue, the court focused on whether the bank's security procedure qualified as "commercially reasonable." Article 4A provides guidance, explaining that "commercial reasonableness" may be determined by reference to, *inter alia*, "the circumstances of the customer known to the bank, including the size, type and frequency of payment orders normally issued by the customer to the bank."[39]

Based on this guidance, the First Circuit found that the bank's conduct undermined its security procedure, rendering it "commercially *unreasonable*."[40] By lowering the threshold to $1 for use of the "challenge questions," the court found that the bank had made the procedure indiscriminate.[41] Apparently accepting Patco's argument, the First Circuit reasoned that because every payment order triggered the "challenge questions," the bank gave the thieves expanded opportunities to use keyloggers "to capture all information necessary to compromise an account."[42] The bank thereby increased "the risk of fraud through unauthorized use of compromised security answers."[43] The bank also failed to diminish that risk with any additional security measures.[44] Additionally, the bank ignored the warnings its own system generated and also failed to notify Patco before it processed the flagged payment orders.[45] The bank could have monitored high-risk-score transactions (but did not); it could have used e-mail for rapid communication of fraud alerts to customers (but used snail mail instead). These collective failures in the bank's security system made it "commercially

35. *Id.*
36. *Id.*
37. *Id.* at 208.
38. *Id.* at 208–09.
39. *Id.*
40. *Id.* at 211.
41. *Id.*
42. *See id.* at 210–11.
43. *Id.* at 210.
44. *See id.*
45. *Id.* at 213.

unreasonable."[46] The First Circuit remanded the case for a determination of "what, if any, obligations or responsibilities are imposed on a commercial customer under Article 4A even where a bank's security system is commercially unreasonable."[47]

Counsel advising on risk-allocating eBanking agreements will find *Patco* instructive on the unobvious limits to such agreements and their dependence on the quality of a bank's implementation of its security procedure. Good security procedures, poorly implemented or undermined by decisions with security consequences that have not been examined or understood, apparently do not provide "commercially reasonable" cybersecurity.

III. When the Federal Government Shares Cyber Intelligence, the Recipients Acquire Responsibilities to Protect It and Make Good, Quick Use of It

On February 12, 2013, President Obama issued Executive Order No. 13636 ("Order") with a strategic objective: to protect national security by safeguarding the nation's critical infrastructure from cyber threats.[48] The Order directs federal agencies to pursue several strategies, including, among others, sharing cyber threat intelligence with critical infrastructure companies.[49] The Order seeks to increase the "volume, timeliness, and quality of cyber threat information shared [by federal agencies] with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats."[50]

How does the Order work? It directs the Attorney General, the Secretary of Homeland Security ("DHS Secretary"), and the Director of National Intelligence, by mid-June 2013, to issue instructions "to ensure the timely production of *unclassified* reports of cyber threats to the U.S. homeland that identify a specific targeted entity."[51] The Order requires the same officials to "establish a process that rapidly disseminates" such reports "to the targeted entity."[52] These reports will put private-sector recipients on formal notice that they are targets of an imminent cyber attack.

The Order sets a deadline of mid-July 2013 for the DHS Secretary to "identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."[53] The Order also requires the DHS Secretary to

46. *Id.* at 211.
47. *Id.* at 215. Subsequent to the First Circuit's decision, defendant People's United Bank agreed to pay plaintiff Patco the total amount of the funds that the hackers had stolen and that had not been recovered by the bank ($345,000), plus approximately $45,000 in interest. Kim Zetter, *Bank Agrees to Reimburse Hacking Victim $300K in Precedent-Setting Case*, Wired (Nov. 30, 2012), http://www.bernsteinshur.com/wp-content/uploads/2012/11/Wired_Mitchell.pdf.
48. Executive Order No. 13636, 78 Fed. Reg. 11737 (Feb. 19, 2013).
49. *Id.* at 11739.
50. *Id.*
51. *Id.* (emphasis added).
52. *Id.* The process will also disseminate "classified reports" to cleared entities.
53. *Id.* at 11742.

"*confidentially* notify owners and operators of critical infrastructure" identified as having such risks "that they have been so identified" and to provide them the basis for that determination.[54] These reports will put recipients on formal notice that a cyberattack on their facilities may well cause "catastrophic" damage regionally or nationally.

Potential recipients may not appreciate the prospect that every cyber intelligence report comes with implicit responsibilities. Because these reports will originate with the federal government, as opposed to being mere rumor, they will put recipients at risk of being judged by stakeholders, regulators, and courts by a thrice-elevated standard. First, recipients will be in a poor position to argue the attack or its damaging consequences were "unforeseeable"—because the federal government put them on notice. Second, stakeholders and potential plaintiffs will ask: did the recipients act responsibly *when they had the brief window of opportunity to react to timely informative intelligence?* Did they promptly use it to improve the preparedness of their cyber defenses, incident responses, and recovery from severe event damage and disruption? Finally, unlike many corporate crises that management may address over a period of days, in a cybersecurity crisis (which may start with receipt of a DHS Secretary's report of an imminent attack or the attack itself), management must be prepared to respond swiftly and responsibly within hours, and preferably within minutes, or may be held accountable for failing to do so.[55]

In short, delivery of cyber intelligence magnifies the recipient's responsibilities by raising the stakes for any failure to address cybersecurity adequately after having been put on notice and given solid cause to do so. The Order's lacunae may limit those magnifying effects. *How detailed and timely will the reports be? What should recipients do with the intelligence? Will DHS respond to recipients seeking clarifications?* On these questions, the Order is no more illuminating than the *Coal Sack* nebula's vast darkness.[56]

IV. Cybersecurity Vulnerabilities Become the Legal Responsibility of Their Designers

For decades, software makers have protected themselves from the consequences of suspected but uncorrected vulnerabilities. They urged buyers to invest in their products' latest enhanced features and capabilities. But they did not mention that they had not thoroughly checked to see if their products contained undiscovered or undisclosed defects and vulnerabilities.

To have discovered them (with extended testing), averted them (with security as a design priority), and corrected them (with code re-written and re-tested)

54. *Id.* (emphasis added).

55. *See* David A. Katz & Laura A. McIntosh, *Cybersecurity Risks and the Board of Directors*, N.Y. L.J., Nov. 29, 2012, at 3, *available at* http://www.wlrk.com/webdocs/wlrknew/AttorneyPubs/WLRK.22213.12.pdf.

56. Aptly named, *Coal Sack* is the most prominent and conspicuous dark nebula in the skies. It extends from the lower left quadrant of *Southern Cross* like a dark hole in the Milky Way star fields. *See* Robin Kerrod, The Star Guide 82 (1997).

would have required tradeoffs in time-to-market and other costs apparently unacceptable to makers. Aware of the broad risks—that malware or targeted cyber attacks could exploit the packaged vulnerabilities to cause widespread harm—the makers shrink-wrapped the risk of such losses to fall on the customer.

Regulators were as aware of these practices as Captain Renault was of practices at *Rick's Café Américain*.[57] But now the FTC has signaled its intent to hold software makers *responsible* for the security of their wares. Under its decision, manufacturers must discover and remove vulnerabilities in their software before they release it.

In February 2013, HTC America, Inc. ("HTC"), a maker of Android-based, mobile devices, entered into a settlement with the FTC. The FTC's complaint alleged HTC failed to "employ reasonable and appropriate security in the design and customization of the software on its mobile devices."[58] The complaint also alleged that HTC failed to (1) implement an "adequate program to assess the security of products it shipped to consumers," (2) provide "adequate privacy and security guidance or training for its engineering staff," (3) "conduct . . . reviews, or tests to identify potential security vulnerabilities in its mobile devices," and (4) "implement a process for receiving and addressing security vulnerability reports from third-party researchers."[59]

Additionally, the Complaint alleged that HTC introduced "permission re-delegation" vulnerabilities in the Android operating system on its devices.[60] "Permission re-delegation" occurs when an application with permission to access *sensitive information* gives another application (without the same level of permission) access to it.[61] Re-delegation enables third parties to circumvent the Android operating system's security. As a result, third parties can operate the device's microphone for audio recording, access "GPS-based, cell-based, and WiFi-based location information," and authorize sending text messages—all without the user's consent.[62] They could surreptitiously (1) record phone conversations, (2) track a user's location, and (3) commit toll fraud ("sending text messages to premium numbers in order to charge fees to the user's phone bill").[63] Thus, third parties could record and transmit financial account numbers and personal identification numbers entered into or stored on HTC devices.[64] The exploitable vulnerabilities reside on "18.3 million HTC devices."[65] Counsel will find the full text of the Complaint deserves study because it details security deficiencies the FTC appears unwilling to let developers leave in products they sell to buyers.

57. *See* Casablanca (MGM 1942).
58. Complaint ¶ 7, *In re* HTC Am., Inc., No. 122-3049, 2013 WL 752478 (FTC Feb. 22, 2013), *available at* http://www.ftc.gov/os/caselist/1223049/130222htccmpt.pdf.
59. *Id.*
60. *Id.* ¶ 9.
61. *Id.*
62. *Id.*
63. *Id.*
64. *Id.* ¶ 16.
65. *Id.* ¶ 11.

In the settlement, HTC agreed to remediation measures, including implementing a comprehensive security program, developing "security patches to fix" vulnerabilities, and periodic third-party assessments of its remediation efforts for twenty years.[66]

V. Conclusion

A year ago, no one imagined that three decisions—*Patco*, Executive Order No. 13636, and the FTC/HTC America settlement—would transform cybersecurity responsibilities. They constitute the *Crux*—the constellation of the year's most significant decisions in cybersecurity law. Each suggests the need for thoughtful responses to escalating cyber threats and attacks. Each signals significant changes in corporate cybersecurity responsibilities.

Though issued in different contexts, these decisions illuminate one another when read together; omit any one of them and one misses the constellation. One thereby loses sight of a valuable navigation aid for businesses engaged in global commerce that the prodigious reach and intensity of cyberattacks have turned into a new *terra incognita*. However, if kept in view, this constellation of decisions provides strong reasons for readers to initiate conversations with officers, directors, owners, and operators of critical infrastructure, financial services providers, and manufacturers of products and software. As these decisions demonstrate, every client's business now depends on cyber-secure communications, transactions, and infrastructure.

66. Agreement Containing Consent Order at 3–5, *In re* HTC Am., Inc., No. 122-3049, 2013 WL 752478 (FTC Feb. 22, 2013), *available at* http://www.ftc.gov/os/caselist/1223049/130222htcorder.pdf.

Developments in Data Security Breach Liability

*By John Black**

Data breaches of personal information continued to grow in number and size in 2012 and 2013 at businesses and governmental agencies in the United States. Throughout 2012, major companies suffered hacking attacks compromising the security of personal data in their possession. Such companies included Global Payments, Inc. in March (at least 1.5 million card numbers),[1] LinkedIn in June (6.4 million user passwords),[2] Barnes & Noble in September (credit card information taken from sixty-three stores),[3] and Nationwide Mutual Insurance in October (1.1 million accounts).[4] Significant breaches continued in early 2013, with Schnucks announcing in March that 2.4 million debit and credit cards used at seventy-nine stores may have been compromised.[5] Government agencies were not immune—in October 2012, the state of South Carolina announced hackers had stolen 3.6 million Social Security numbers and 387,000 credit/debit card numbers from its Department of Revenue, seemingly affecting more than 75 percent of the state's population.[6]

---

* John Black is a principal with Boundas, Skarzynski, Walsh & Black, LLC, in Chicago, where he counsels clients on legal issues involving technology, media, data security and privacy, and insurance coverage for such risks. He is an active member of the Cyberspace Law Committee, appearing on a December 2012 ABA Business Law Section Webinar: *Insuring for Data Security Threats: Everything a Business Lawyer Wants to Know but Is Afraid to Ask*. Mr. Black is also a coauthor of the *Information Security* chapter in INTERNET LAW FOR THE BUSINESS LAWYER (Juliet M. Moringiello ed., 2d ed. 2012). Mr. Black can be reached at jblack@bswb.com.

1. Info. Sec. Media Grp., *Global Payments Breach Tab: $94 Million*, BANK INFO. SEC. (Jan. 10, 2013), http://www.bankinfosecurity.com/global-payments-breach-tab-94-million-a-5415/op-1.

2. Nicole Perlroth, *Lax Security at LinkedIn Is Laid Bare*, N.Y. TIMES (June 10, 2012), http://goo.gl/DRAf0M.

3. Michael S. Schmidt & Nicole Perlroth, *Credit Card Data Breach at Barnes & Noble Stores*, N.Y. TIMES (Oct. 23, 2012), http://goo.gl/Nplwx.

4. Antone Gonsalves, *Nationwide/Allied Security Breach Highlights Litigation Fears*, CSO ONLINE (Dec. 7, 2012), http://www.csoonline.com/article/723378/nationwide-allied-security-breach-highlights-litigation-fears.

5. Georgina Gustin, *Schnucks Breach Happened When Cards Were Awaiting Approval*, ST. LOUIS POST-DISPATCH (Apr. 15, 2013, 5:41 PM), http://goo.gl/guz03g.

6. Lucian Constantin, *South Carolina Reveals Massive Data Breach*, PC WORLD (Oct. 27, 2012), http://www.pcworld.com/article/2013186/south-carolina-reveals-massive-data-breach.html; *see* U.S. Census Bureau, *State & County Quick Facts: South Carolina*, CENSUS (June 27, 2013, 1:52 PM), http://quickfacts.census.gov/qfd/states/45000.html (estimating the 2012 population of South Carolina at 4,723,723).

The number of reported data breaches increased in 2012 from 2011, and 2013 is on pace to surpass 2012.[7]

Businesses face substantial out-of-pocket costs for breach events, often including consulting fees for forensic investigation and remediation, legal fees, cost of providing notification to affected customers, credit monitoring costs, public relations fees, and costs of settling litigation or government investigations, including fines and penalties. According to a survey by the Ponemon Institute, the average cost of a data breach in 2012 was $5.4 million, or $188 per record.[8] The direct costs for detection and escalation, notification, and other response expenses (including legal fees) averaged $2.36 million.[9] Not surprisingly, the damage to a company's reputation and business may also be significant—a substantial portion of the average cost of a data breach was attributed to lost business ($3.03 million).[10]

Lack of Damages Remains a Roadblock for Most Civil Data Breach Class Actions

Major data breaches often are followed by litigation on behalf of affected consumers. Through 2012 and early 2013, plaintiffs' attorneys continued to be active in pursuing data breach class actions on behalf of consumers seeking damages for the unauthorized loss or disclosure of personal information. These class actions typically include claims of unfair competition, negligence, invasion of privacy, breach of express or implied contract, bailment, and violation of consumer protection laws.

However, these lawsuits generally struggle to survive motions to dismiss on the ground that they do not adequately allege standing under Article III of the U.S. Constitution or the requisite damages for the pleaded causes of action. For example, in December 2011, the Third Circuit upheld the dismissal of a class action by employees who worked for companies that used Ceridian Corporation to process company payrolls, finding that indefinite risks of future harm and mitigation costs were too speculative to give the plaintiffs standing under Article III.[11]

Article III standing requires that a plaintiff show an injury in fact, a causal connection between the injury and the conduct complained of, and that the injury will likely be redressed by a favorable decision.[12] An "injury in fact" may include

7. According to the Identity Theft Resource Center, U.S. companies and governmental agencies reported 419 breaches in 2011, 470 breaches in 2012, and 469 breaches through October 14, 2013. *See* Identity Theft Res. Ctr., 2013 Breach List 1 (Oct. 14, 2013), *available at* http://www.idtheftcenter.org/images/breach/ITRC_Breach_Report_2013.pdf; Identity Theft Res. Ctr., 2012 Breach List 1 (Jan. 4, 2013), *available at* http://www.idtheftcenter.org/images/breach/Breach_Report_2012.pdf; Identity Theft Res. Ctr., 2011 Breach List 1 (Feb. 7, 2012), *available at* http://www.idtheftcenter.org/images/breach/Breach_Report_2011.pdf.

8. Ponemon Inst., 2013 Cost of Data Breach Study: Global Analysis 1, 5 (May 2013). The study included fifty-four U.S. companies in sixteen industries. *Id.* at 1, 4.

9. *See id.* at 16–17.

10. *Id.* at 17.

11. Reilly v. Ceridian Corp., 664 F.3d 38, 40–43 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2395 (2012).

12. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992).

the invasion of a legally protected interest that is concrete and particularized, and actual or imminent (i.e., not conjectural or hypothetical).[13] In actions for loss of personal data, a frequent issue has been whether the possibility of future injury in the absence of actual harm is enough to satisfy the Article III "injury in fact" requirement.[14]

Recently, some courts have been more willing to recognize that consumer plaintiffs have an increased risk of future injury or otherwise sustained mitigation costs sufficient under Article III to support an actionable claim.[15] Plaintiffs' attorneys have also increasingly sought to avoid the injury restrictions of Article III by pleading the violation of federal statutes that do not have an injury requirement, such as the Wiretap Act[16] or the Stored Communications Act,[17] or that provide liquidated damages, such as the Video Privacy Protection Act.[18] The basis for asserting federal statutory claims that do not have an injury requirement as a means to avoid Article III standing requirements is rooted in the Ninth Circuit's decision in *Edwards v. First American Corp.*,[19] in which the court stated that the "injury required by Article III can exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'"[20] Thus, for example, the district court in *In re iPhone Application Litigation*[21] recently held that "a violation of the Wiretap Act or the Stored Communications Act may serve as a concrete injury for the purposes of Article III injury analysis."[22]

In September 2012, the Eleventh Circuit in *Resnick v. AvMed, Inc.*[23] held that the alleged use of stolen personal information to open accounts and make unauthorized purchases was a sufficient harm resulting from the loss of the personal information to permit a customer class action to survive a motion to dismiss based on Article III standing. In *Resnick*, the customer plaintiffs alleged that two unencrypted laptops containing their personal information were stolen from AvMed's corporate offices, resulting in their personal information being used to open accounts and make unauthorized purchases.[24] The circuit court overturned the district court's dismissal of the action, holding the plaintiffs adequately alleged "actual identity theft resulting from a data breach"[25] traceable to the defendant's actions and the plaintiffs' monetary losses were cognizable under Florida law.[26] The court affirmed that their claims for negligence per se,

13. *Id.* at 560.
14. *Reilly*, 664 F.3d at 43.
15. *See, e.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1141–43 (9th Cir. 2010); Ruiz v. Gap, Inc., 380 F. App'x 689, 690–91 (9th Cir. 2010).
16. 18 U.S.C. §§ 2510–2522 (2012).
17. 18 U.S.C. §§ 2701–2712 (2012).
18. 18 U.S.C. § 2710.
19. 610 F.3d 514 (9th Cir. 2010).
20. *Id.* at 517 (indirectly quoting Warth v. Seldin, 422 U.S. 490, 500 (1975)).
21. 844 F. Supp. 2d 1040 (N.D. Cal. 2012).
22. *Id.* at 1055.
23. 693 F.3d 1317 (11th Cir. 2012).
24. *Id.* at 1322.
25. *Id.* at 1323.
26. *Id.* at 1327–28.

negligence, breach of contract, breach of the covenant of good faith and fair dealing, and unjust enrichment/restitution satisfied federal pleading requirements, but held that each of the claims of negligence per se and breach of the implied covenant of good faith and fair dealing failed to allege entitlement to relief under Florida law.[27]

In October 2012, the district court granted in part Sony's motion to dismiss customer claims in the multi-district class action involving the 2011 PlayStation Network data breach.[28] The court found that the plaintiffs had "articulated sufficient particularized and concrete harm to sustain a finding of injury-in-fact at this stage in the pleadings"[29] because they alleged "their sensitive Personal Information was wrongfully disseminated, thereby increasing the risk of future harm."[30] While the risk of future harm to the plaintiffs from the exposure of their personal data was sufficient under Article III, the court nevertheless determined that the harm was too speculative to state a claim of negligence under California law.[31] The court granted leave to file an amended complaint,[32] and the plaintiffs filed an amended complaint in early December.[33]

In March 2013, the district court dismissed a class action complaint brought on behalf of paid subscribers to LinkedIn whose e-mail addresses and passwords had been compromised in a hack attack.[34] The plaintiffs argued they had standing to sue under a theory of economic harm, contending they did not receive the full benefit of their bargain for their paid premium memberships.[35] They alleged that LinkedIn promised to secure their personal information "with industry standard protocols and technology,"[36] and without such a promise they would not have purchased premium memberships.[37] The court recognized that economic harm based on the "benefit of the bargain" is a viable basis for Article III standing, but rejected that the plaintiffs did not gain the benefit of their bargain.[38] The court observed that the user agreement and privacy policy were identical for premium and non-paying memberships, and that the benefit for which members purchased a premium account was not the promise of enhanced security but

27. *See id.* at 1328–30. The court held AvMed was not subject to the statute that formed the basis for the negligence per se count, *id.* at 1328–29, and the plaintiffs failed to allege AvMed's failures to secure their data resulted from a "conscious and deliberate act, which unfairly frustrate[d] the agreed common purpose," *id.* at 1329, as required to state a claim for breach of the implied covenant of good faith and fair dealing under Florida law. *Id.*

28. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 950–52 (S.D. Cal. 2012).

29. *Id.* at 958.

30. *Id.*

31. *Id.* at 962–63.

32. *Id.* at 975.

33. First Amended Consolidated Class Action Complaint, *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942 (S.D. Cal. 2012) (No. 3:11-md-02258-AJB-MDD).

34. *In re* LinkedIn User Privacy Litig., 932 F. Supp. 2d 1089, 1090–92 (N.D. Cal. 2013).

35. *Id.* at 1092–93.

36. *Id.* at 1093.

37. *Id.*

38. *Id.*

more advanced networking tools.[39] The court concluded that this was not a "case where consumers paid for a product, and the product they received was different from the one as advertised on the product's packaging."[40] The plaintiffs therefore were required to allege "something more" than pure economic harm from overpaying for a defective product, which might include the theft of personally identifiable information.[41] The most that could be shown here was that one plaintiff's LinkedIn password was "posted on the Internet on June 6, 2012."[42] Accordingly, the court dismissed the claims for lack of a legally cognizable injury.[43]

Other consumer data breach class actions have also foundered on state law requirements to plead cognizable present or future damages. In February 2012, the Oregon Supreme Court in *Paul v. Providence Health System-Oregon*[44] upheld the dismissal of a class action data breach complaint on the ground that the mere threat of future harm was insufficient to sustain a claim for negligence or violation of the Unlawful Trade Practices Act.[45] The complaint alleged the plaintiffs suffered economic and noneconomic damages when computer disks and tapes containing personal information from 365,000 patients were stolen from the car of a Providence employee.[46] The trial court and the court of appeals held that plaintiffs had failed to state claims, and the Oregon Supreme Court affirmed because, absent allegations that the stolen information was used or even viewed by a third party, the plaintiffs did not suffer a cognizable injury.[47]

Similarly, in November 2012, the district court dismissed a class action against a video game developer, Valve Corporation ("Valve"), for failing to plead cognizable present or future damages based on subscriber information—including billing addresses, passwords, online IDs, and credit card information—taken by a hacker in November 2011.[48] The plaintiffs alleged they lost access to Valve's service, data, and the benefit of their bargain, and that they might be forced to spend money to "protect their privacy."[49] The court held that, in light of the size and potential expense of the class action, the alleged present damages were insufficient.[50] Moreover, the mere possibility the plaintiffs might be forced to spend money to protect their privacy was not cognizable in the absence of "actual fraud or identity theft."[51] However, the court granted leave to file an amended complaint.[52]

39. *Id.*
40. *Id.* at 1094.
41. *Id.*
42. *Id.*
43. *Id.* at 1095.
44. 273 P.3d 106 (Or. 2012).
45. *Id.* at 114–15.
46. *Id.* at 107.
47. *Id.* at 107–08.
48. Grigsby v. Valve Corp., No. C12-0553JLR, 2012 WL 5993755, at *1 (W.D. Wash. Nov. 14, 2012).
49. *Id.* at *2.
50. *Id.* at *4.
51. *Id.* at *2.
52. *Id.* at *5.

Data Breach Class Certification Hurdles

With most privacy class action complaints failing to survive a motion to dismiss, there have been few opportunities for class certification issues to be addressed. On March 20, 2013, the district court's denial of a motion for class certification in *In re Hannaford Brothers Co. Customer Data Security Breach Litigation* provided new guidance on this issue.[53] The court determined that the plaintiffs did not meet the predominance requirement under Federal Rule of Civil Procedure 23(b)(3),[54] which requires a plaintiff to show that "questions of law or fact common to class members *predominate* over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy."[55]

Hannaford arose from the theft of 4.2 million debit and credit card numbers and other customer information between December 2007 and March 2008 from a grocery store chain's computer network.[56] Affected customers filed a putative class action in 2008 against Hannaford Brothers Company ("Hannaford") alleging seven causes of action as a result of the breach.[57] After extensive motions before several courts including the Maine Supreme Court[58] and the First Circuit,[59] the claims against Hannaford were reduced to negligence and breach of implied contract, with the damages limited to the only cognizable injury pleaded by the plaintiffs, out-of-pocket expenditures customers made in reasonable attempts to mitigate economic injury.[60]

On the class certification issue, the district court ruled that the plaintiffs satisfied the Rule 23(a) requirements of numerosity, commonality, typicality, and adequacy,[61] but concluded they did not show that common questions of law or fact predominated over questions affecting only individual members.[62] The court recognized that the complaint presented common questions of liability concerning whether Hannaford breached a duty to maintain its customers' credit and debit card information securely and whether that breach caused the intrusion, affected the plaintiffs' electronic data, and reasonably led the plaintiffs to take protective measures that cost money.[63] Focusing on practical issues concerning how the trial might work if the case proceeded as a class action, the court determined the plaintiffs did not meet their burden of showing predominance with respect to the actual impact on particular cardholders, such as

53. No. 2:08-MD-1954-DBH, 2013 WL 1182733 (D. Me. Mar. 20, 2013).
54. *Id.* at *8–10.
55. Fed. R. Civ. P. 23(b)(3) (emphasis added).
56. *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 4 A.3d 492, 494 (Me. 2010).
57. *Id.*
58. *Id.* (resolving question certified by federal district court on customers' motion).
59. Anderson v. Hannaford Bros. Co., 659 F.3d 151 (1st Cir. 2011).
60. *See id.* at 167 (reversing dismissal of negligence and implied contract claims and affirming dismissal of remaining claims).
61. *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., No. 2:08-MD-1954-DBH, 2013 WL 1182733, at *2–8 (D. Me. Mar. 20, 2013) (applying Fed. R. Civ. P. 23(a)(1)–(4)).
62. *Id.* at *8–10.
63. *Id.* at *8.

whether their particular accounts suffered fraudulent charges, and the mitigating steps the plaintiffs took and the costs they incurred.[64] The court rejected the plaintiffs' argument that the trial would be straightforward because they would show by statistical proof the total lump sum damages, noting that in such cases "the plaintiffs already had an expert who had looked at the data and stated his/her ability to testify what the total damages would be."[65] Observing that the plaintiffs failed to present any expert opinion testimony stating that total damages could be proven by statistical methods, but only asserted such testimony could be found, the court concluded the plaintiffs had failed to establish "predominance."[66]

While the district court in *Hannaford* indicated that expert proof likely may be necessary in data breach class action claims to establish predominance of damages and causation, an April 2013 decision by the U.S. District Court for the Northern District of Illinois suggests such proof may not be necessary in a privacy class actions for improper collection of personal data. In *Harris v. comScore, Inc.*,[67] the court certified a putative privacy class action for allegedly improper collection of personal information. The defendant, comScore, Inc. ("comScore"), collected data about the internet activities of consumers, analyzed the data, and sold the information to its clients.[68] The class action complaint alleged that comScore "developed highly intrusive and robust data collection software . . . to surreptitiously siphon exorbitant amounts of sensitive and personal data from consumers' computers,"[69] and used "deceitful tactics to disseminate its software and . . . gain constant monitoring access to millions of . . . computers and networks."[70] By using such software, comScore allegedly collected a "terrifying"[71] amount of data from "unsuspecting customers,"[72] including usernames, passwords, and credit card numbers, all allegedly violating the Stored Communications Act, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, as well as constituting unjust enrichment.[73]

The court granted class certification as to the plaintiffs' statutory claims, ruling that the plaintiffs satisfied the requirements for class certification under Federal Rule of Civil Procedure 23, including predominance.[74] However, a key difference from *Hannaford* may be that the Stored Communications Act and the Electronic Communications Privacy Act provide for statutory damages, as the court rejected comScore's predominance argument that there were individualized

64. *See id.* at *9.
65. *Id.* at *10.
66. *Id.*
67. No. 11 C 5807, 2013 WL 1339262, at *1 (N.D. Ill. Apr. 2, 2013).
68. *Id.*
69. Class Action Complaint ¶ 4, Harris v. comScore, Inc., No. 11 C 5807, 2013 WL 1339262 (N.D. Ill. Apr. 2, 2013).
70. *Id.*
71. *Id.* ¶ 7.
72. *Id.*
73. *Id.* ¶¶ 7, 84–113, 120–24.
74. Harris v. comScore, Inc., No. 11 C 5807, 2013 WL 1339262, at *5–10 (N.D. Ill. Apr. 2, 2013).

issues as to whether each plaintiff suffered damage or loss.[75] Although the Computer Fraud and Abuse Act permits civil actions only for persons who suffer damage or loss aggregating to at least $5,000 in a single year,[76] the court held it would be more efficient to resolve all common issues in a single proceeding.[77]

What Is Commercially Reasonable Security?

As most data breach class actions have been dismissed for lack of damages, courts generally have not examined what might constitute reasonable data security when plaintiffs allege negligence. Although several states have data security laws that require businesses to adopt reasonable security measures to protect personal information,[78] of which the most notable and comprehensive may be Massachusetts Regulation 17,[79] those statutes do not define what constitutes reasonable data security.[80] However, in a different context, the First Circuit recently addressed reasonable security under Article 4A of the Uniform Commercial Code. In a case that likely will have wide ranging implications for financial institutions and perhaps other businesses, the court in *Patco Construction Co. v. People's United Bank*[81] held that a bank failed to provide commercially reasonable security to protect a customer from fraud.[82] The security procedures proved commercially unreasonable, in part, because the bank posed the same challenge questions for high-risk transactions that it did for ordinary transactions, which was particularly troubling given the prevalence of key-logging malware, about which the bank had been cautioned by its consultants.[83]

In the wake of *Patco*, other bank customers have brought actions for alleged failures by their banks to provide commercially reasonable security. For example, in April 2013, Oregon Hay Products, Inc. ("Oregon Hay") filed a complaint in state court against Community Bank for allegedly violating Article 4A of the U.C.C. by permitting unauthorized wire transfers from its bank account.[84] According to the complaint, commercially unreasonable security procedures at the bank allowed wire transfers totaling $223,500 to be sent from Oregon

75. *Id.* at *10.

76. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I), (g) (2012).

77. *Harris*, 2013 WL 1339262, at *10.

78. *See, e.g.*, Ark. Code Ann. § 4-110-104(b) (West Supp. 2013); Cal. Civ. Code § 1798.81.5(b) (Deering 2005 & Supp. 2013); Md. Code Ann., Com. Law § 14-3503 (LexisNexis 2013); Mass. Gen. Laws ch. 93H, § 2(a) (2012); Nev. Rev. Stat. Ann. § 603A.210 (West Supp. 2013); Or. Rev. Stat. § 646A.622 (2011); R.I. Gen. Laws Ann. § 11-49.2-2 (West 2006); Tex. Bus. & Com. Code Ann. § 521.052(a) (West 2009 & Supp. 2013); Utah Code Ann. § 13-44-201 (West 2010).

79. 201 Mass. Code Regs. 17.01–17.05 (2012).

80. *Compare* Or. Rev. Stat. § 646A.622(2) (setting forth general safe harbors deemed to constitute "reasonable safeguards").

81. 684 F.3d 197 (1st Cir. 2012).

82. *Id.* at 210–13.

83. *See id.* at 211.

84. Complaint, Or. Hay Prods., Inc. v. Cmty. Bank, No. CVH120083 (Or. Cir. Ct. Apr. 11, 2012) (alleging violation of Or. Rev. Stat. § 74A.2020, Oregon's version of section 202 of Article 4A of the U.C.C.).

Hay's checking account to a bank in the Ukraine over a three-day period.[85] The complaint alleged the wire transfers were initiated from different IP addresses that Oregon Hay had not previously used, were sent to a bank account to which Oregon Hay had never before transferred funds, and were of a size, type, and frequency unlike those normally issued by Oregon Hay.[86] Moreover, the wire transfers were initiated on three consecutive dates on an account in which Oregon Hay had only initiated eight wire transfers in the prior year.[87]

Concluding Observations

With the prevalence of large-scale data breaches, class action data breach litigation appears unlikely to disappear any time soon. Indeed, the ever increasing use of technology to store, access, and transfer personal information for business and personal reasons, coupled with the rapid development and adoption of such technology, suggests that large-scale data breaches of personal information will continue unabated. At the same time, persons aggrieved by the potential misuse of their personal information or harmed by the actual misuse of that information, aided by a creative plaintiffs' bar, do not lack incentives to seek remedies for potential and actual harms flowing from unauthorized use of their personal information. Courts have been grappling with issues of standing, the cognizability of injuries, and whether plaintiffs adequately pleaded their claims, threshold issues that appear likely to continue to be a major focus in data breach litigation. However, as case law develops on these issues and some data breach class actions survive initial motions to dismiss, courts are beginning to address other issues, including damages and the appropriateness of class certification, which may emerge as a new battleground in data breach litigation.

85. *See id.* ¶¶ 7, 16.
86. *See id.* ¶ 16.
87. *See id.*

2013 State of the Law Regarding Internet Intermediary Liability for User-Generated Content

*By Catherine R. Gellis**

I. Introduction

In the past year the law relating to intermediaries continued to be shaped and further solidified by judicial process. Increasingly, however, we are seeing extra-judicial efforts to redefine its contours, as meanwhile courts sometimes struggle to apply existing law to new legal challenges.

This survey primarily focuses on recent jurisprudence interpreting the two major statutes governing intermediary liability: 47 U.S.C. § 230 ("Section 230")[1] and 17 U.S.C. § 512 (the "DMCA").[2] Intermediaries are also affected by other ancillary legal constructs, and this survey touches on some of them as well. For simplicity, the intermediaries discussed are generally websites hosting content created by their users, although other sorts of intermediaries are at times discussed as their jurisprudence can also be instructive.[3]

II. Intermediary Liability Generally

Section 230 handles most of the heavy lifting when it comes to intermediary liability, providing that "[n]o 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."[4] As an example, while newspapers are responsible for the articles they write and publish online, they are not legally responsible for the comments readers post to them.[5]

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

1. 47 U.S.C. § 230 (2012).

2. 17 U.S.C. § 512 (2012). Section 512 was enacted as part of the Digital Millennium Copyright Act, Pub. L. No. 105-304, § 202(a), 112 Stat. 2860, 2877 (1998).

3. As with prior years' surveys on the subject, cases involving keyword advertising will be omitted, even though the subject frequently implicates questions of intermediary liability, as that body of case law is worthy of separate treatment.

4. 47 U.S.C. § 230(c)(1) (2012).

5. *See* Hadley v. GateHouse Media Freeport Holdings, Inc., No. 12 C 1548, 2012 WL 2866463, at *2 (N.D. Ill. July 10, 2012).

This immunity remains even when they exert some editorial control over these comments.[6]

Consumer review sites are also frequently immunized under Section 230, even when they have exerted some editorial control over how user-posted content appears on their sites.[7] Similarly, search engines that link to content created by a third party are likewise immunized.[8] In general, Section 230 precludes liability for anyone linking to content created by another, even if that content is defamatory,[9] just as there is no liability, as courts have continued to make clear over the past year, for hosting content directly as long as the content was created by a third party.[10]

6. *See*, *e.g.*, Gains v. Romkey, No. 11-0594, 2012 WL 7007002, at *5 (Ill. App. Ct. July 3, 2012) ("[E]ditors for the Moline Dispatch were assigned to moderate the comments submitted by others to the website in order to assure the comments were not abusive, obscene, profane, or otherwise offensive. . . . However, other than screening these comments, the editors did not modify the comments prepared by third parties or contribute to the content whatsoever. Defendants merely disseminated the comments made by third parties. As such, under section (c) of the Act, defendants do not qualify as the speaker or publisher of information provided by a third party . . . , but are merely the interactive computer service which enables access by multiple users, as defined under section (f)(2) of the Act. . . ."). *Compare* Ascend Health Corp. v. Wells, No. 4:12-CV-00083-BR, 2013 WL 1010589, at *8 (E.D.N.C. Mar. 14, 2013) (denying a Section 230 defense at the motion to dismiss stage to assess whether a site owner's interaction with third-party-posted content made it an information content provider rather than an immune interactive computer services provider).

7. *See*, *e.g.*, Seaton v. TripAdvisor, LLC, No. 3:11-CV-549, 2012 WL 3637394, at *7 (E.D. Tenn. Aug. 22, 1012) (holding it was legitimate for TripAdvisor to rank "dirtiest hotels" based on the reviews posted by others, although not on Section 230 grounds); *see also* Courtney v. Vereb, No. 12-655, 2012 WL 2405313, at *5 (E.D. La. June 25, 2012) (finding a party who distributed user-generated content via fax or telephone could still qualify as an immune provider of interactive computer services as defined by 47 U.S.C. § 230(f)(2)). *But see* Vo Grp., LLC v. Opinion Corp., No. 8758/11, slip op. at 9–10 (N.Y. Sup. Ct. May 22, 2012) (denying a motion to dismiss on Section 230 grounds after finding a question of authorship in the content in question, as well as an issue of potential extortion raised by how the "Pissed Consumer" website offered to remove negative posts in exchange for payment), *available at* http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1073&context=historical.

8. *See*, *e.g.*, Getachew v. Google, Inc., 491 F. App'x 923, 926 (10th Cir. 2012) ("Google cannot be held liable for search results that yield content created by a third party."); Mmubango v. Google, Inc., No. 12-1300, 2013 WL 664231, at *3 (E.D. Pa. Feb. 22, 2013) ("Google cannot be held liable for state law defamation on the facts that it 'decided' to publish a third party's statements, which has been identified by the Third Circuit as a traditional editorial function."); Nieman v. Versuslaw, Inc., No. 12-3104, 2012 WL 3201931, at *8 (C.D. Ill. Aug. 3, 2012) (concluding that state law claims of defamation and invasion of privacy are barred by Section 230); Shah v. MyLife.com, Inc., No. 3:12-cv-1592-ST, 2012 WL 4863696, at *3 (D. Or. Sept. 21, 2012) ("[D]efendants cannot be sued for simply republishing information provided by third parties . . . .").

9. *See*, *e.g.*, Shrader v. Beann, 503 F. App'x 650, 654 (10th Cir. 2012); Directory Assistants, Inc. v. Supermedia, LLC, 884 F. Supp. 2d 446, 452 (E.D. Va. 2012); Vazquez v. Buhl, No. FSTCV126012693S, 2012 WL 3641581, at *4 (Conn. Super. Ct. July 17, 2012).

10. *See*, *e.g.*, Klayman v. Zuckerberg, 910 F. Supp. 2d 314, 319–21 (D.D.C. 2012); Merritt v. Lexis Nexis, No. 12-12903, 2012 WL 6725881, at *1 (E.D. Mich. Dec. 27, 2012). *But see* Nasser v. WhitePages, Inc., No. 5:12cv097, 2013 WL 2295678, at *4 (W.D. Va. May 24, 2013) (finding discovery was required to determine if a website that published an incorrect phone number supplied by someone else qualified as an immune service provider); *see also* Lansing v. Sw. Airlines Co., 980 N.E.2d 630, 632, 639–41 (Ill. App. Ct. 2012) (holding Section 230 does not protect an employer from a negligent supervision claim for an employee's use of defendant's computer, internet, and telephone facilities to send harassing e-mails and texts to plaintiff).

Significantly, the immunity provision of Section 230 preempts state law that might otherwise provide a right of action against an internet service provider.[11] In cases with difficult facts and sympathetic victims, however, state courts and legislatures have sometimes ignored this preemption provision. For instance, a Texas court summarily denied, in a one-sentence order, a motion to dismiss predicated on Section 230 filed by GoDaddy.com, the host of a "revenge porn" website that hosted explicit pictures of identifiable women without their permission.[12] Meanwhile, the State of Washington proposed a law, Senate Bill 6251, that would make "it a felony to knowingly publish, disseminate, or display or to 'directly or indirectly' cause content to be published, disseminated or displayed if it contain[ed] a 'depiction of a minor' and any 'explicit or implicit offer' of sex for 'something of value.'"[13] The bill would, a federal court later found, affect online intermediaries like Backpage.com that host online ads.[14] Thus, the federal district court enjoined its enforcement due to it being prempted by Section 230.[15]

III. Intermediary Liability with Regard to Copyright

Section 230 does contain a few exceptions to the immunity it generally provides intermediaries, most notably for claims relating to intellectual property.[16] When those claims relate to copyright, compliance with the DMCA's requirements can instead provide the intermediary with a "safe harbor" insulating it from having hosted its users' potentially infringing content.[17]

This past year saw further developments to two notable appellate decisions in the Ninth and Second Circuits from the previous year regarding the DMCA's safe harbors. In *UMG Recordings, Inc. v. Shelter Capital Partners LLC*,[18] the Ninth Circuit, following a denial of an en banc rehearing, issued a decision superseding its

11. 47 U.S.C. § 230(e)(2) (2012) ("No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."). On the other hand, in *Sulla v. Horowitz*, No. 12-00449 SOM/KSC, 2012 WL 4758163 (D. Haw. Oct. 4, 2012), the federal court found that "[Section] 230 is clearly in the nature of a defense [and] therefore does not provide this court with federal question jurisdiction." *Id*. at *2.

12. *See* Toups v. Godaddy.com, No. D-130,018-C, slip op. at 1, (D. Tex. Apr. 17, 2013) (order denying motion to dismiss) ("After reading the authorities presented to the court and considering the arguments of counsel, it is my opinion that the Motion to Dismiss should be denied at this time.").

13. Backpage.com, LLC v. McKenna, 881 F. Supp. 2d 1262, 1268 (W.D. Wash. 2012).

14. *See id*. In an earlier case, Backpage.com had been found entitled to Section 230 immunity for the content of user-posted ads, in spite of the ads' potential to involve sexual exploitation of minors. M.A. v. Vill. Voice Media Holdings, LLC, 809 F. Supp. 2d 1041, 1058 (E.D. Mo. 2011).

15. Backpage.com, LLC v. McKenna, No. C12-954 RSM, 2012 WL 4120262, at *2 (W.D. Wash. Sept. 18, 2012). Rulings like this have now prompted some state attorneys general to lobby Congress to amend Section 230 such that it no longer immunizes intermediaries from criminality manifest in their users' content as recognized under state law. *See* Elizabeth Heichler, *U.S. States' Attorneys General to Take Aim at Internet 'Safe Harbor' Law*, TechHive (June 18, 2013), http://www.techhive.com/article/2042351/us-states-attorneys-general-to-take-aim-at-internet-safe-harbor-law.html.

16. 47 U.S.C. § 230(e)(2) (2012).

17. The DMCA describes several safe harbors covering a variety of types of intermediaries. The provision most applicable to the discussion here is 17 U.S.C. § 512(c).

18. 718 F.3d 1006 (9th Cir. 2013), *superseding* 667 F.3d 1022 (9th Cir. 2011). For further discussion of this court's interpretation of the safe harbor requirements, see Catherine R. Gellis, *2012*

prior ruling,[19] although this new decision largely left in place its previous conclusion that the intermediary had been entitled to DMCA safe harbor protection for videos its users had posted to it.[20] In *Viacom International, Inc. v. YouTube, Inc.*,[21] the Second Circuit had previously remanded the case to the district court to determine whether "YouTube had knowledge or awareness of any specific infringements," which would make it ineligible for the safe harbor if it did not delete them, or, if YouTube did not have such knowledge, whether it "willfully blinded itself to [such knowledge]," which would also make it ineligible.[22] The district court had also been tasked with determining "[w]hether YouTube had the 'right and ability to control' infringing activity within the meaning of § 512(c)(1)(B)," and "[w]hether any clips-in-suit were syndicated to a third party and, if so, whether such syndication occurred 'by reason of the storage at the direction of the user' within the meaning of § 512(c)(1), so that YouTube may claim the protection of the § 512(c) safe harbor."[23]

On the first points, the district court dismissed Viacom's argument that the potentially infringing content hosted by YouTube was so voluminous that Viacom should be spared from having to send notices for each allegedly infringing clip, finding that the burden to police for infringements remained with Viacom and would not be shifted to YouTube.[24] Furthermore, while a service provider like YouTube was ordinarily relieved of a duty to police infringements as long as it acted to delete them when it became aware of specific instances, merely having a general idea that it might be hosting infringing content, without knowing where it was hosted, did not constitute "willful blindness" as to the infringement, which would have disqualified YouTube from the safe harbor.[25]

Regarding the "right and ability to control," the court ruled that "the governing principle must remain clear: knowledge of the prevalence of infringing activity, and welcoming it, does not itself forfeit the safe harbor. To forfeit that, the provider must influence or participate in the infringement."[26] Here, the court said:

> There is no evidence that YouTube induced its users to submit infringing videos, provided users with detailed instructions about what content to upload or edited their content, prescreened submissions for quality, steered users to infringing videos,

State of the Law Regarding Internet Intermediary Liability for User-Generated Content, 68 BUS. LAW. 289, 293–94 (2012).

19. *UMG Recordings*, 718 F.3d at 1010.

20. *Id.* at 1031.

21. Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012).

22. *Id.* at 42.

23. *Id.* In the wake of the *YouTube* appellate ruling, the district court in *Capitol Records, Inc. v. MP3Tunes, LLC* granted in part the plaintiff's motion to reconsider an earlier summary judgment ruling and referred for trial questions concerning willful blindness and "red flag" knowledge. Capitol Records, Inc. v. MP3tunes, LLC, No. 07 Civ. 9931(WHP), 2013 WL 1987225, at *2–4 (S.D.N.Y. May 14, 2013), *rev'g in part* 821 F. Supp. 2d 627 (S.D.N.Y. 2011).

24. Viacom Int'l, Inc. v. YouTube, Inc., No. 07 Civ. 2103 (LLS), 2013 WL 1689071, at *3 (S.D.N.Y. Apr. 18, 2013).

25. *Id.* at *4–5.

26. *Id.* at *6.

> or otherwise interacted with infringing users to a point where it might be said to have participated in their infringing activity.[27]

Thus, "YouTube did not have the right and ability to control infringing activity within the meaning of § 512(c)(1)(B)."[28]

Finally, the court also found that automatically encoding the content YouTube hosted so that downstream providers could deliver it across various devices did not convert the content from having been "stor[ed] at the direction of . . . user[s]"[29] into content attributable to YouTube.[30] On the contrary, providing the encoding merely helped "provid[e] access to material stored at the direction of users," as a service provider was entitled to do under § 512(c).[31]

Last year intermediaries were also protected from liability in *Obodai v. Demand Media, Inc.*, which involved a website that expeditiously removed user-posted material when notified it was infringing,[32] and in *Luvdarts, LLC v. AT&T Mobility, LLC* a mobile telephone service provider avoided liability for infringing content transmitted by those using the service.[33] However, in *Columbia Pictures Industries, Inc. v. Fung*, the defendant was found ineligible for a safe harbor under subsection 512(a),[34] (c),[35] or (d).[36] While defendants in *Shelter Capital* and *YouTube* that simply hosted the content alleged to be infringing, in *Fung* the defendant did not host any content but instead ran several BitTorrent tracking sites that allegedly helped users upload and download infringing content hosted on other computers.[37] Borrowing heavily from the reasoning in *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*,[38] the court found the defendant liable for inducing third parties to download infringing copies of copyrighted works, even though it did not find the defendant liable for direct infringement.[39] The court then extended the logic by which it found the defendant liable for inducement to also find it ineligible for the DMCA safe harbors,[40] even though the

27. *Id.* at *9.
28. *Id.*
29. 17 U.S.C. § 512(c)(1) (2012).
30. *Viacom Int'l*, 2013 WL 1689071, at *10.
31. *Id.* (quoting Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 40 (2d Cir. 2012)).
32. No. 11 Civ. 2503 (PKC), 2012 WL 2189740 (S.D.N.Y. June 13, 2012), *aff'd sub nom.* Obodai v. Cracked Entm't Inc., No. 12-2450, 2013 WL 2321420 (2d Cir. May 29, 2013).
33. 710 F.3d 1068 (9th Cir. 2013).
34. 710 F.3d 1020, 1040–42 (9th Cir. 2013).
35. *Id.* at 1042–46.
36. *Id.* at 1046–47.
37. *Id.* at 1028–29.
38. 545 U.S. 913 (2005).
39. *Columbia Pictures Indus.*, 710 F.3d at 1031–39.
40. *Id.* at 1040–47. On the other hand, in *Flava Works, Inc. v. Gunter*, 689 F.3d 754 (7th Cir. 2012), the court found that a "social bookmarking" website that allows users to link to videos hosted elsewhere on the internet and then embed them in the website's user interface did not make the website secondarily liable for infringement. *See id.* at 762; *see also* Routt v. Amazon.com, Inc., No. C12-1307JLR, 2012 WL 5993516, at *3 (W.D. Wash. Nov. 30, 2012) (holding Amazon not vicariously liable for its affiliates' alleged infringements).

court then found that the DMCA safe harbors could potentially protect a service provider against claims of vicarious, as well as direct, liability for infringement.[41]

Several other recent cases have also tested the limits of the DMCA. In *Perfect 10, Inc. v. Yandex N.V.*, the court discussed the sufficiency of takedown notices[42] and reiterated the importance of having a registered DMCA agent as described by § 512(c)(2) in order to be eligible for the safe harbor at all.[43] Perhaps more significant, however, was the result in *UMG Recordings, Inc. v. Escape Media Group, Inc.*, a case involving the Grooveshark music service, where a New York state court found DMCA safe harbors unavailable for potential infringements of pre-1972 sound recordings under the reasoning that the DMCA is part of the federal copyright law and pre-1972 sound recordings are protected only by state copyright law.[44]

IV. Other Intermediary Liability Issues

While most Section 230 and DMCA jurisprudence has been steadily developing as described above, intermediaries continue to face other legal challenges. For instance, in *Pirozzi v. Apple Inc.*, Apple successfully moved to dismiss a claim to hold it liable for the privacy practices of developers of Apple-compatible apps,[45] and Alibaba avoided liability for the bad conduct of the merchants that it certified,[46] although neither did so on Section 230 grounds. The past year also saw several cases addressing the question of whether someone running an open WiFi connection could be liable for the copyright infringement in content that a user of that WiFi connection transmitted.[47]

Intermediaries also often find themselves in the line of fire by parties wishing to hold their users accountable when those users are anonymous. For copyright infringement allegations, the DMCA allows intermediaries to be subpoenaed for the identifying information of these suspected users.[48] Recent cases involving a high-volume copyright litigant, however, suggest that this provision can be abused.[49] Notably, a court recently determined that the First Amendment does not provide

41. *See* 17 U.S.C. § 512 (2012); *Columbia Pictures Indus.*, 710 F.3d at 1045–46.

42. No. C 12-01521 WHA, 2013 WL 1899851, at *3–6 (N.D. Cal. May 7, 2013).

43. *Id.* at *7–8.

44. 964 N.Y.S.2d 106, 109–11 (App. Div. 2013).

45. 913 F. Supp. 2d 840, 848–52 (N.D. Cal. 2012).

46. Englert v. Alibaba.com H. K. Ltd., No. 4:11CV1560 RWS, 2012 WL 1468472, at *3 (E.D. Mo. Apr. 27, 2012).

47. *See*, *e.g.*, AF Holdings, LLC v. Doe, No. C 12-2049 PJH, slip op. at 3–4 (N.D. Cal. Sept. 4, 2012) (finding no duty to secure a WiFi connection); *see also* Liberty Media Holdings, LLC v. Tabora, No. 12 Civ. 2234 (LAK), 2012 WL 2711381, at *1–2 (S.D.N.Y. July 9, 2012) (rejecting attempts to find a defendant negligent for sharing an internet connection with another who allegedly infringed on plaintiff's copyright).

48. 17 U.S.C. § 512(h) (2012).

49. *See*, *e.g.*, Brief of Electronic Frontier Foundation et al. as Amici Curiae Supporting Appellants at 3–5, AF Holdings, LLC v. Does 1–1,058, No. 12-7135 (D.C. Cir. May 14, 2013), *available at* https://www.eff.org/node/74213 (describing boilerplate complaints filed against thousands of holders of internet accounts). Note, however, that the subpoenas used in these cases were issued pursuant to the Federal Rules of Civil Procedure, and not the DMCA. See *id.* at 10-11.

grounds to quash these DMCA subpoenas.[50] For non-DMCA subpoenas, however, the normal rules of civil procedure will apply.[51]

The DMCA also has limits. While its safe harbor protects intermediaries from damages for copyright infringement in content created by others, no law clearly protects intermediaries against claims of potential trademark infringement in user-created content, which results in intermediaries potentially having to defend themselves in trademark cases arising from their users' content.[52]

Even with regard to copyright, recent cases suggest a disconnect between civil infringement liability, against which the DMCA would protect an intermediary, and criminal infringement liability, for which its safe harbors are unavailable.[53] This past year Richard O'Dwyer, a student in England who began the TVShack website that hosted links to TV shows found on the internet, reached a settlement with the Department of Justice, which had been trying to extradite him to the United States to face criminal charges of copyright infringement based on having hosted those links.[54] Meanwhile, the Department of Justice has continued its attempts to extradite Kim Dotcom from New Zealand to face similar charges for his Megaupload website that had hosted user-posted video.[55]

V. Conclusion

Ultimately this past year has seen Section 230 and DMCA jurisprudence continue to stabilize around some core questions, but it will take more time to discover just how far courts and legislatures will let their protections extend.

50. *See* Signature Mgmt. Team, LLC v. Automattic, Inc., No. C-13-80028 RCB, 2013 WL 1739480, at *8–10 (N.D. Cal. Apr. 22, 2013).

51. *See* Brompton Building, LLC v. Yelp!, Inc., No. 1-12-0547, 2013 WL 416185, at *1–6 (Ill. App. Ct. Jan. 31, 2013) (disallowing a litigious landlord claiming defamation to subpoena the identity of a Yelp! reviewer).

52. *See* Born to Rock Design Inc. v. CafePress.com, Inc., No. 10 Civ. 8588 (CM), 2012 WL 3954518 (S.D.N.Y. Sept. 7, 2012). *But see* DeVere Grp. GmbH v. Opinion Corp., 877 F. Supp. 2d 67, 74 (E.D.N.Y. 2012) (dismissing claim of trademark infringement against operator of consumer complaint website); Tre Milano, LLC v. Amazon.com, Inc., No. B234753, 2012 WL 3594380, at *7–14 (Cal. Ct. App. Aug. 22, 2012) (applying Tiffany (NJ) Inc. v. eBay, Inc., 600 F.3d 93 (2d Cir. 2010) to exonerate Amazon.com given how it had responded to notices that its third party marketplace sellers were dealing in counterfeit merchandise).

53. *See*, *e.g.*, 17 U.S.C. § 512(c)(1) (2012) ("A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief . . . .").

54. *See 'Piracy' Student Richard O'Dwyer Avoids US Extradition*, BBC News (Nov. 28, 2012), http://www.bbc.co.uk/news/uk-england-south-yorkshire-20525891.

55. *See* Eriq Gardner, *Kim Dotcom Case to Be Reviewed by New Zealand's Supreme Court,* Hollywood Rep. (May 16, 2013), http://www.hollywoodreporter.com/thr-esq/kim-dotcom-case-be-reviewed-524004.

Privacy in the Age of Big Data

*By John Pavolotsky**

"Big Data" is here. In fact, soon Big Data will be small data.[1] Gartner defines Big Data as "high-volume, -velocity and -variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making."[2] In essence, Big Data refers to the proliferation in data volumes and types, the dramatic increase in the speed for collecting and processing that data, and the technical solutions to analyze, store, and draw intelligent and actionable inferences from the data. Big Data is premised on intensive data mining on large and diverse data sets, which may be online, offline, or a combination of the two. The rise in unstructured data (free-form text, video, voice, etc.) and machine data (web, server, application, and database logs; sensor data from medical devices, smart meters, and appliances), cheaper storage, web services, and the ubiquity of broadband access in many corners have all played a large role in the emergence of Big Data. Technical solutions include Apache Hadoop,[3] an open source software platform that enables, among other things, the parallel processing of large data sets. Big Data and related technologies have been applied in a number of industries, including retail,[4] healthcare,[5] insurance,[6] automotive,[7]

* John Pavolotsky, CIPP-US is a technology attorney based in northern California.

1. *See* Patrick Tucker, *Has Big Data Made Anonymity Impossible?*, MASHABLE (May 7, 2013), http://mashable.com/2013/05/07/big-data-anonymity/ (noting a 2,000 percent projected increase in global data by 2020).

2. Svetlana Sicular, *Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three "V"s*, FORBES (Mar. 27, 2013, 8:00 AM), http://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/.

3. *See* APACHE HADOOP, http://hadoop.apache.org/ (last visited Aug. 25, 2013).

4. *See* Jeff Bertolucci, *Big Data Helps Retailers Target Mobile Customers*, INFO.WEEK (Apr. 4, 2013), http://www.informationweek.com/big-data/news/big-data-analytics/big-data-helps-retailers-target-mobile-c/240152281.

5. *See* John Markoff, *Unreported Side Effects of Drugs Are Found Using Internet Search Data, Study Finds*, N.Y. TIMES (Mar. 6, 2013), http://www.nytimes.com/2013/03/07/science/unreported-side-effects-of-drugs-found-using-internet-data-study-finds.html?_r=0.

6. *See* Clint Boulton, *Auto Insurers Bank on Big Data to Drive New Business*, WALL ST. J. (Feb. 20, 2013, 5:03 PM), http://blogs.wsj.com/cio/2013/02/20/auto-insurers-bank-on-big-data-to-drive-new-business/.

7. *See* Derrick Harris, *How Data Is Changing the Car Game for Ford*, USA TODAY (Apr. 29, 2013, 9:36 AM), http://www.usatoday.com/story/tech/2013/04/29/data-ford-gigaom/2120481/.

entertainment,[8] and publishing.[9] More ominous applications include cell-phone tracking,[10] the proposed creation of a national biometric database,[11] and drones.[12] Thus, while Big Data creates many benefits, it raises a number of issues, including those relating to data privacy. This survey focuses on the privacy issues raised by Big Data and suggests risk mitigation techniques.

I. Big Data Jurisprudence

At a minimum, courts are beginning to acknowledge Big Data. For example, one court noted: "First, in the era of 'big data,' in which storage capacity is cheap and several bankers' boxes of documents can be stored with a keystroke on a three inch thumb drive, there are simply more documents that everyone is keeping and a concomitant necessity to log more of them."[13] Another court noted that a certain Big Data analytics market "consists of companies that use data mining techniques to derive insights from the flow of information generated on" a particular social networking site.[14] As discussed below, other courts, while not using the term Big Data, have nonetheless tackled issues, such as geolocational privacy, raised by Big Data technologies. In particular, these courts have examined the collection and use of GPS data, from both traditional GPS transponders and GPS chips in mobile phones, and cell site data by law enforcement officials in connection with surveillance operations.

United States v. Jones[15] involved a GPS device that had been attached to the undercarriage of the defendant's car. The GPS device tracked the location of Mr. Jones's car for twenty-eight consecutive days, relaying more than 2,000 pages of data.[16] While Justice Scalia's majority opinion ultimately disposed of the case based on a common law trespass analysis,[17] Justice Alito, in a concurring opinion joined by three other Justices, provided that prolonged monitoring of a person's whereabouts for most offenses would violate a person's reasonable expectation of privacy and, therefore, be unconstitutional, absent a warrant or exigent circumstances.[18] Although Justice Sotomayor penned a separate concur-

8. *See* David Carr, *Giving Viewers What They Want*, N.Y. Times (Feb. 24, 2013), http://www.nytimes.com/2013/02/25/business/media/for-house-of-cards-using-big-data-to-guarantee-its-popularity.html?pagewanted=all&_r=0.

9. *See* Alexandra Alter, *Your E-Book Is Reading You*, Wall St. J., July 19, 2012, at D1, *available at* http://online.wsj.com/article/SB10001424052702304870304577490950051438304.html.

10. *See, e.g.*, United States v. Skinner, 690 F.3d 772 (6th Cir. 2012).

11. *See* David Kravets, *Biometric Database of All Adult Americans Hidden in Immigration Reform*, Wired (May 10, 2013, 6:30 AM), http://www.wired.com/threatlevel/2013/05/immigration-reform-dossiers/.

12. *See* Robert Beckhusen, *White House 'Big Data' Push Means Big Bucks for Drone Brains*, Wired (Mar. 29, 2012, 5:13 PM), http://www.wired.com/dangerroom/2012/03/big-data/.

13. Chevron Corp. v. Weinberg Grp., 286 F.R.D. 95, 98–99 (D.D.C. 2012).

14. PeopleBrowsr, Inc. v. Twitter, Inc., No. C-12-6120 EMC, 2013 WL 843032, at *1 (N.D. Cal. Mar. 6, 2013).

15. 132 S. Ct. 945 (2012).

16. *Id.* at 948.

17. *See id.* at 949–50.

18. *Id.* at 964 (Alito, J., concurring).

ring opinion, she nonetheless seemed to agree with Justice Alito's reasoning.[19] In view of the foregoing, it seems likely that the Court will continue to apply the "reasonable expectation of privacy" test first articulated by Justice Harlan in *Katz v. United States*[20] to tracking technologies. Further, relatively recent advancements in tracking technologies, which allow location data to be collected without attaching a physical device to the property of the person being tracked, call into question the utility of a common law trespass analysis in future cases.

United States v. Skinner[21] involved a GPS-enabled cell phone that was pinged periodically for three days. Law enforcement officials used location data collected from the phone to apprehend the defendant, who subsequently filed a motion to suppress, arguing that a warrant based on probable cause should have been obtained before any data were gathered.[22] The U.S. Court of Appeals for the Sixth Circuit concluded that "Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone."[23] While Judge Donald, in her concurring opinion, disagreed with the majority's rationale, she nonetheless concluded that the location data evidence should not be suppressed because a good-faith exception to the warrant requirement existed.[24]

Courts have also examined the constitutionality of warrantless searches based on the collection of cell-site data. Put simply, wireless carriers record the locations of the nearest cell towers at the beginning and end of a phone call made on a mobile device.[25] With such data, the location of a device can be determined with reasonable accuracy.[26] Interestingly, relying on the Court's favorable ruling in *United States v. Jones*,[27] Mr. Jones petitioned the U.S. District Court for the District of Columbia to suppress cell-site data gathered during a four-month period pursuant to three separate orders issued by magistrate judges.[28] In particular, Jones argued that such data could not be collected without a warrant based on probable cause.[29] There, the court denied the defendant's motion to suppress, because, in its view, the good-faith exception to the exclusionary rule applied.[30] Notably, the court discussed in great detail the constitutionality of

19. *See id.* at 954–57 (Sotomayor, J., concurring). Perhaps more important, Justice Sotomayor intimated the need to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Id.* at 957.

20. 389 U.S. 347, 361 (1967) (Harlan, J., concurring). In particular, Justice Harlan, in his concurring opinion, stated: "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.*

21. 690 F.3d 772 (6th Cir. 2012).

22. *See id.* at 774–75.

23. *Id.* at 777.

24. *See id.* at 786–88 (Donald, J., concurring).

25. *See* United States v. Jones, 908 F. Supp. 2d 203, 206–07 (D.D.C. 2012).

26. *See id.*

27. 132 S. Ct. 945 (2012).

28. *Jones*, 908 F. Supp. 2d at 204.

29. *Id.*

30. *Id.*

collecting cell-site data without a warrant based on probable cause, but, as noted above, was able to avoid a determination because "exclusion is not required 'when the police act with an objectively reasonable good-faith belief that their conduct is lawful.'"[31]

II. Big Data and FIPs

For most practicing attorneys, the issues raised by government surveillance cases are of limited applicability, but the issues loom large for any practitioner who represents the government, the defendant whose location data have been collected by law enforcement officials, or a state actor. While other attorneys need not face these issues, they still must be aware of the privacy issues, as detailed below, raised by Big Data.

As noted, Big Data is founded on comprehensive data collection and extreme data analytics, which guide the use and/or disclosure of the data. Modern privacy law is based on fair information practices (FIPs), principles that address the rights of individuals, controls on the information, and the collection, use and storage, and disclosure of the information.[32] Individuals' rights consist of notice, choice and consent, and access.[33]

Notice and consent are problematic, particularly so for Big Data. Many consumers do not read privacy policies, which are often inscrutable to lawyers and non-lawyers alike. Privacy policies displayed on devices, such as cell phones, with small-form factors are at best difficult to read, and layered notices, providing a brief summary of the privacy terms with a link to the full privacy policy, are often unavailable. Notices should be clear and state the purpose for which personal data will be collected, used, disclosed, and retained. In the case of Big Data, prospective identification of the data-collection purposes may be challenging because an organization cannot realistically anticipate what the data will reveal until after intensive data mining is complete.

Put otherwise, even if an individual read and understood a privacy policy, that policy may be wrong or at least incomplete. Again, Big Data, the value of which lies in identifying secondary (and thus unimagined) uses of data, stretches the practical limits of meaningful consent. Moreover, the entity collecting data may transmit it to another, thereby losing control over its ultimate use. Further, a direct relationship might not exist between a data subject and the organization that stores his or her personal information. Consider, for example, data brokers, which collect, combine, and sell (or license) data from online and offline sources for marketing and other purposes.[34] In practical terms, individuals would have no way of knowing who ultimately uses their data or how it ultimately might be used.

31. *Id.* at 214 (citing Davis v. United States, 131 S. Ct. 2419, 2427 (2011)).

32. *See Fair Information Practice Principles*, Fed. Trade Comm'n, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last modified Nov. 23, 2012).

33. *See id.*

34. *See infra* Part IV.A.

III. Anonymization

One of the foundational concepts in modern privacy law is anonymization or de-identification.[35] As applied to data, this involves masking or obfuscating data to prevent individual identification. In the European Union, personal data relates to an identified or identifiable individual.[36] If data is effectively anonymized, the EU Data Protection Directive would not apply.[37] The same concept applies to U.S. data privacy laws, such as the Health Insurance Portability and Accountability Act of 1996[38] and, in particular, the Privacy Rule thereunder, the latter of which allows de-identification of personal health information through an "Expert Determination" method (which requires the application of statistical or scientific principles to determine the risk of identification) and "Safe Harbor" method (which involves removing eighteen types of identifiers and requiring the absence of actual knowledge that the information could be used to identify an individual).[39] In addition, to comply with state data breach statutes,[40] organizations routinely obfuscate data. Big Data and related techniques challenge and in some instances re-identify previously de-identified data. Put simply, with the availability of even bigger data sets and more robust analytics, there are sometimes only a few hops between de-identified data and the identity of a particular individual. For example, researchers at MIT and the Université Catholique de Louvain (Belgium) analyzed data on 1.5 million cellphone users residing in a small European county and found that they could identify 95 percent of such users based on only four points of reference.[41] Thus, the Big Data tsunami should prompt companies to review their de-identification protocols, ensure that these protocols are being implemented properly, and reconsider if certain data should simply not be collected from individuals.

IV. The FTC and Big Data

A. Data Brokers

The Federal Trade Commission ("FTC") has been active in pursuing data brokers regarding potential privacy issues and, in particular, potential violations of the Fair Credit Reporting Act ("FCRA").[42] On May 7, 2013, the FTC announced that it recently had conducted a "shopping operation," showing that a number of

35. *See generally* Neil M. Richards, *The Perils of Social Reading*, 101 Geo. L.J. 689, 711–12 (2013) (discussing anonymity as foundational to privacy in the context of social reading).

36. *See* Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data art. 2(a), 1995 O.J. (L 281) 31 (defining "personal data").

37. *See id*. art. 3 (defining the scope of the directive).

38. *See* 42 U.S.C. § 1320d-2 (2012) (requiring the Secretary to adopt security standards and safeguards).

39. *See* 45 C.F.R. § 164.514(b) (2013).

40. *See, e.g.*, *Privacy Laws*, Office of the Att'y Gen., State of Cal. Dep't of Justice, http://oag.ca.gov/privacy/privacy-laws (last visited Sept. 6, 2013) (collecting California's privacy laws).

41. *See* Larry Hardesty, *How Hard Is It to 'De-Anonymize' Cellphone Data?*, MIT News Office (Mar. 27, 2013), http://web.mit.edu/newsoffice/2013/de-anonymize-cellphone-data-0327.html.

42. *See* 15 U.S.C. §§ 1681–1681x (2012).

companies may be operating as consumer reporting agencies and, as such, would be subject to the FCRA.[43] In particular, the FTC sent letters to ten such companies, noting potential violations, including failures to confirm that the purchasers of the consumer lists and other consumer information offered by these data brokers would use them only for permissible purposes.[44] Clearly, the FTC is setting the stage for a long battle with data brokers.[45] Previously, and to no avail, the FTC had called for legislative oversight of data brokers and, in particular, legislation to require data brokers to identify to individuals whether personal data are held by them with respect to the individuals.[46] In 2012, the FTC announced that, for $800,000, it had settled claims that Spokeo, a data broker that compiles and sells information profiles, operated as a consumer reporting agency and violated the FCRA by, among other things, failing to ensure that the profiles were used for lawful purposes.[47]

B. Privacy by Design

While Privacy by Design ("PBD") is not a new concept, it was expressly and fully embraced by the FTC in its 2012 report titled *Protecting Consumer Privacy in an Era of Rapid Change*.[48] In essence, PBD provides that organizations, at every stage of a product's design and development, should build in consumer privacy protections, such as reasonable security, limited data collection and retention, and reasonable procedures to achieve data accuracy.[49] In February 2013, a leading mobile device manufacturer settled FTC charges that it failed to use reasonable security practices when it developed software for its smartphones and tablets.[50] The resulting security flaws, in the FTC's view, could have put at risk sensitive information about millions of customers.[51] Notably, while charges

43. Press Release, Fed. Trade Comm'n, FTC Warns Data Broker Operations of Possible Privacy Violations (May 7, 2013), http://www.ftc.gov/opa/2013/05/databroker.shtm.

44. *Id*.

45. *See* Craig Timberg, *FTC Warns Data Brokers on Privacy Rules*, Wash. Post (May 7, 2013), http://articles.washingtonpost.com/2013-05-07/business/39090758_1_data-brokers-personal-data-data-reports.

46. Edward Wyatt, *F.T.C. and White House Push for Online Privacy Laws*, N.Y. Times (May 9, 2012), http://www.nytimes.com/2012/05/10/business/ftc-and-white-house-push-for-online-privacy-laws.html?_r=0.

47. Press Release, Fed. Trade Comm'n, Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA (June 6, 2012), http://www.ftc.gov/opa/2012/06/spokeo.shtm. For more on this and other FTC actions, see Fatima Nadine Kahn, *Survey of Recent FTC Privacy Enforcement Actions and Developments*, 69 Bus. Law. 227 (2013).

48. *See* Press Release, Fed. Trade Comm'n, FTC Issues Final Commission Report on Protecting Consumer Privacy (Mar. 26, 2012), *available at* http://www.ftc.gov/opa/2012/03/privacyframework.shtm.

49. Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 23–30 (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

50. Press Release, Fed. Trade Comm'n, HTC America Settles FTC Charges It Failed to Secure Millions of Mobile Devices Shipped to Consumers (Feb. 22, 2013), http://www.ftc.gov/opa/2013/02/htc.shtm.

51. *See id*.

relating to security were asserted under the unfairness prong of section 5 of the FTC Act,[52] clearly the FTC had PBD in mind when prescribing the proactive implementation of reasonable data security measures.[53] The importance of data security is heightened by the volume of data collected, as well as by the nature of the data. Thus, Big Data technologies and practices should stress PBD and cause any organization to think twice about what personal data it collects, how it secures that data, and how it can integrate robust security protections as the product is being designed and developed.

C. Do Not Track

While Do Not Track ("DNT") is at the top of the FTC's agenda,[54] given disagreements regarding technical implementation and continuing debate over the value proposition for Big Data at the consumer level, it is unlikely that there will be any progress with any DNT legislation anytime soon. Put simply, DNT would be a federally mandated opt-out regime as applied to an individual's search and other internet activities.[55] Note that DNT generally focuses on tracking and not on the underlying collection of consumer data. Put otherwise, even if DNT legislation were passed in some form, there would still likely be massive amounts of data collected, which, as noted above, presents considerable security concerns.

V. Proposed Legislation

Not surprisingly, members of Congress have introduced a variety of bills that attempt to deal with the privacy issues raised by technologies that fall within the realm of Big Data. For example, on September 12, 2012, Representative Markey introduced the Mobile Device Privacy Act.[56] Pursuant to this proposed legislation, which has since died, organizations would have needed to disclose monitoring software installed on a mobile device or downloadable to such a device, the types of information that could be collected by such software, the recipients of such information, how such information would be used, and procedures to stop further collection of such information.[57] Further, the bill had somewhat detailed information security requirements for anyone that receives information collected by monitoring software, including a security policy, the identification of a security officer, and a process for identifying any reasonably foreseeable vulnerabilities in any system containing such information.[58] More recently, proposed legislation includes the Electronic Communications Privacy Act Amend-

52. 15 U.S.C. § 45 (2012).
53. *See* Press Release, Fed. Trade Comm'n, *supra* note 50.
54. *See* Jessica Guynn, *FTC Calls on Online Ad Industry to Agree on Do-Not-Track Standard*, L.A. Times (Apr. 17, 2013, 3:41 PM), http://www.latimes.com/business/technology/la-fi-tn-ftc-online-ad-industry-do-not-track-20130417,0,5397711.story.
55. *See id*.
56. *See* H.R. 6377, 112th Cong. § 3 (2012).
57. *See id*. § 2.
58. *See id*. § 4.

ments Act of 2013,[59] which was introduced by Senator Leahy. More broadly, Congress is concerned about the requirements for seeking geolocational data and drawing a distinction, if warranted, between particular tracking technologies, namely GPS and cell-tower data.[60]

VI. Risk Mitigation

In view of the Big Data tsunami, what options are available to organizations to steer clear of potential violations of data privacy laws and for consumers to ensure that reasonable expectations of privacy are in fact being met? For organizations, risk mitigation begins with the development of a comprehensive and realistic privacy plan. In contrast to a privacy policy, a privacy plan is directed internally toward those in the company who will have access to consumer data. Organizations should embrace Privacy by Design, and many have already subscribed to its tenets, by setting privacy as the default.

Companies should devote greater attention to the development of privacy policies that are simpler and more specific to actual products or services and an organization's collection, use, disclosure, and storage of data in connection with that product or service. Put otherwise, because no two businesses are the same, if privacy policies are the same or substantially similar, at least one of the privacy policies is not on point. Big Data and related technologies should cause organizations to refocus their attention on the flow of data in connection with a specific product or service, and if the collected data is to be used for a context different from, or incompatible with, the one for which it was first collected, the consumer should be required to consent to that new use. Ultimately, the notice-and-consent model is based on control, and a consumer cannot control what she or he does not know or cannot reasonably understand.

The situation for organizations using or providing Big Data solutions to other companies is quite different. Business customers, depending on negotiating power, can in many instances have the relevant contract override any otherwise applicable Terms of Service or Privacy Policy documents posted on the service provider's website. Customers can mitigate risk by performing business, technical, and legal due diligence on the Big Data solution. As a practical matter, in many instances, the provider will not accept any liability for personal data and will require the customer to indemnify it if any personal data are provided to it, whether intentionally or inadvertently. The only options for the customer are to encrypt the personal data or to scrub the data, which may present an issue operationally. In practice, whether a vendor accepts any liability for data privacy or security is ultimately a function of negotiating power. While an indemnity is preferable, a damages claim may suffice, so long as it is not subject to a limitation-

59. S. 607, 113th Cong. (2013) (reported by Sen. Leahy with an amendment on Apr. 25, 2013); S. 607, 113th Cong. (2013) (originally introduced by Sen. Leahy on Mar. 19, 2013).

60. *See* Press Release, Judiciary Comm., Statement of Judiciary Committee Chairman Bob Goodlatte (Apr. 25, 2013), *available at* http://judiciary.house.gov/news/2013/04252013.html.

of-liability cap, and it is expressly provided that the vendor is responsible for all notification and remediation costs associated with the breach.

Other risk mitigation options include professional liability insurance with cybersecurity coverage. Practitioners should also consider proposing periodic data audits to ensure that the data is being processed, transferred, stored, destroyed, and, in some cases, as necessary, retained, consistent with the customer's litigation hold policies.

Survey of Recent FTC Privacy Enforcement Actions and Developments

*By Fatima N. Khan**

Introduction

In the past few years, the Federal Trade Commission ("FTC") has sharpened its focus on consumer privacy concerns presented by businesses in an environment of rapidly advancing technology. This survey continues from last year's survey,[1] describing major developments by the FTC to address consumer privacy, including enforcement actions, reports, and other agency initiatives.

FTC Enforcement Actions

HTC America, Inc.

In its action against HTC America, Inc. ("HTC"), the FTC focused on reasonable data security in the design and customization of software on mobile devices and its effect on consumer privacy.[2] Among other things, HTC undermined the permission-based model of data collection through its pre-installed applications by (i) failing to include a simple "permission check" code that could prevent a third party from accessing applications without requesting the necessary permissions;[3] (ii) facilitating the downloading of applications outside of the normal installation process, thus bypassing user information and consent protections;[4] (iii) utilizing insecure communications mechanisms in implementing logging applications, placing sensitive information at risk;[5] and (iv) failing to deactivate a debug code that transferred sensitive information and made it accessible to others.[6] Such security risks put consumers at harm by exposing them to malware attacks and potential harms to their financial and personal well-being.[7] These

* Fatima N. Khan is legal counsel at Velti Inc., a mobile marketing company.

1. Fatima N. Khan, *Survey of Recent FTC Privacy Enforcement Actions and Developments*, 68 Bus. Law. 225 (2012).
2. Complaint, *In re* HTC Am., Inc., No. 122-3049, 2013 WL 752478 (FTC Feb. 22, 2013).
3. *Id.* at *2.
4. *Id.*
5. *Id.* at *3.
6. *Id.* at *4.
7. *Id.* at *5.

security risks affecting consumer privacy were also contrary to the representations made by HTC concerning its products.[8]

In its consent order, the FTC (i) enjoined HTC from misrepresenting the security, privacy, confidentiality, or integrity of information from or about consumers, (ii) required HTC to establish a comprehensive security program, and (iii) required HTC to develop security patches to fix the vulnerabilities.[9]

Path, Inc.

In the action against Path, Inc. ("Path"), the FTC and the United States addressed notice, choice, and the Children's Online Privacy Protection Act ("COPPA").[10] Path is a mobile application-based social networking service.[11] Contrary to its privacy policy, Path automatically collected and stored personal information from users' mobile devices on multiple occasions, thereby failing to provide adequate notice.[12] Path also provided illusory user interface options to govern the collection and storage of personal information from the user's mobile device; as a result, users did not have any meaningful choice to protect their personal information.[13] Although it is a general audience application, Path also knowingly accepted registrations from users under age thirteen in violation of COPPA.[14]

In the consent decree and order, the court enjoined Path from improperly collecting information from children online, required Path to delete children's personal information, and imposed a civil penalty of $800,000.[15] Nor may Path misrepresent the extent to which it protects the privacy of covered information, and it must clearly and prominently disclose the categories of information that it will access and/or collect, and obtain the user's affirmative, express consent to do so.[16] Path was also ordered to establish a privacy program and obtain assessments from third-party professionals.[17]

8. *Id.* at *5–6.

9. Agreement Containing Consent Order, *In re* HTC Am., Inc., No. 122-3049, 2013 WL 752478, at *9–10 (FTC Feb. 22, 2013).

10. Complaint for Civil Penalties, Permanent Injunction, and Other Relief, United States v. Path, Inc., C 13 0448 (N.D. Cal. Jan. 31, 2013), *available at* http://www.ftc.gov/os/caselist/1223158/130201pathinccmpt.pdf.

11. *Id.* ¶ 7.

12. *See id.* ¶¶ 15–17.

13. *See id.*

14. *See id.* ¶¶ 18–29.

15. Consent Decree and Order for Civil Penalties, Permanent Injunction and Other Relief ¶¶ 16–21, United States v. Path, Inc., 3:13-cv-00448-RS (N.D. Cal. Feb. 8, 2013), *available at* http://www.ftc.gov/os/caselist/1223158/130201pathincdo.pdf.

16. *Id.* ¶¶ 22–23.

17. *Id.* ¶¶ 24–25; *see also* Consent Decree and Order for Civil Penalties, Injunction, and Other Relief ¶¶ 13–20, United States v. Artist Arena LLC, 1:12-cv-07386-JGK (S.D.N.Y. Oct. 3, 2012), *available at* http://www.ftc.gov/os/caselist/1123167/121003artistarenadecree.pdf (imposing $1 million civil penalty and remedial action for COPPA violation).

Cbr Systems, Inc.

In its action against Cbr Systems, Inc. ("Cbr"), the FTC again demonstrated concern about data security practices affecting personal information, this time in a business involving the collection and storage of umbilical cord blood and tissue.[18] Contrary to its privacy and security representations, Cbr failed to provide reasonable and appropriate security for consumers' personal information by actions such as transporting files of personal information in a manner vulnerable to theft, failing to make backup tapes indecipherable, and failing to destroy no longer needed personal information.[19]

In the decision and order against Cbr, the FTC enjoined Cbr from misrepresenting the extent to which it protects the privacy, confidentiality, security, or integrity of personal information collected from or about consumers.[20] It also required Cbr to create an information security program and obtain biennial assessments from a third-party professional.[21]

Filiquarian Publishing, LLC

In its action against Filiquarian Publishing, LLC, Choice Level, LLC, and Joshua Linsk, an officer of both companies (collectively, "Filiquarian"), the FTC focused on privacy violations of the Fair Credit Reporting Act ("FCRA").[22] Filiquarian provided a mobile application that enabled users to conduct searches for reports on criminal records within states and counties.[23] It did not inquire about the purpose for which any user accessed such reports, but the application contained a disclaimer that purported to shift responsibility for FCRA compliance to the user.[24] The FTC (i) prohibited Filiquarian from furnishing consumer reports to third parties in violation of the guidelines set out in the FCRA and (ii) required it to maintain reasonable procedures to ensure accuracy and limit inappropriate disclosures.[25]

18. Complaint, *In re* Cbr Sys., Inc., No. 112-3120, 2013 WL 391859, at *1–2 (FTC Jan. 28, 2013).

19. *Id.* at *2–3.

20. *In re* Cbr Sys., Inc., No. 112-3120, slip op. at 2 (FTC Apr. 29, 2013) (decision and order), *available at* http://www.ftc.gov/os/caselist/1123120/130503cbrdo.pdf. *Compare* Complaint, *In re* Cbr Sys., Inc., No. 112-3120, 2013 WL 391859, at *13–19 (FTC Jan. 28, 2013) (proposing Agreement Containing Consent Order).

21. *In re* Cbr Sys., Inc., No. 112-3120, slip op. at 3–4 (FTC Apr. 29, 2013) (decision and order), *available at* http://www.ftc.gov/os/caselist/1123120/130503cbrdo.pdf.

22. Complaint, *In re* Filiquarian Publ'g, LLC, No. 112-3195, 2013 WL 205427 (FTC Jan. 10, 2013).

23. *Id.* at *2.

24. *Id.*

25. *In re* Filiquarian Publ'g, LLC, No. 112-3195, slip op. at 3–4 (FTC Apr. 30, 2013) (decision and order), *available at* http://www.ftc.gov/os/caselist/1123195/130501filquariando.pdf. *Compare* Complaint, *In re* Filiquarian Publ'g, LLC, No. 112-3195, 2013 WL 205427, at *4–9 (FTC Jan. 10, 2013) (proposing Agreement Containing Consent Order).

Epic Media Group, LLC

The FTC demonstrated concern for notice and transparency in tracking activities for online behavioral advertising in its action against Epic Marketplace, Inc. and Epic Media Group, LLC (collectively, "Epic").[26] Epic engaged in "history sniffing"—capturing whether a consumer had visited any of over 54,000 domains and assigning an interest segment to that consumer.[27] This practice allowed Epic to circumvent cookie deletion, which is the most common way to prevent tracking, and to capture websites visited not within its inventory.[28] Epic failed to disclose history sniffing in its privacy policy, representing that it only collected information from those websites within its inventory.[29] In its decision and order, the FTC prohibited Epic from misrepresenting privacy and data collection, and from using history sniffing, and it required Epic to delete all data collected using history sniffing.[30]

PLS Financial Services, Inc.

The FTC and the United States took action against PLS Financial Services, Inc., PLS Group, Inc., and The Payday Loan Store of Illinois, Inc. (operating as a common enterprise, "PLS") regarding data security and notice to consumers in the context of payday loan operations.[31] PLS operated loan and check cashing stores in multiple states, collecting sensitive information from consumers, including consumer credit reports, Social Security numbers, and other sensitive information.[32] PLS disseminated to consumers privacy notices that claimed compliance with federal regulations, but its practices contradicted those notices by failing to provide reasonable and appropriate security.[33] According to the FTC, PLS violated (i) the FCRA by failing to dispose properly of consumer information, (ii) the "Safeguards Rule" of the Gramm-Leach-Bliley Act ("GLBA") by failing to protect that information, and (iii) the "Privacy Rule" of GLBA by failing to provide consumers with adequate privacy notices.[34]

26. Complaint, *In re* Epic Marketplace, Inc., No. 112-3182, 2013 WL 1248257 (FTC Mar. 13, 2013).

27. *Id.* at *1–2. The practice was discovered by researchers at the Center for Internet and Society at Stanford Law School, who had posted their research findings online. *See id.* at *2.

28. *Id.* at *2.

29. *Id.* at *2–3.

30. *In re* Epic Marketplace, Inc., No. 112-3182, 2013 WL 1248257, at *3–6 (FTC Mar. 13, 2013) (decision and order).

31. Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief, United States v. PLS Fin. Servs., Inc., No. 1:12-cv-08334 (N.D. Ill. Oct. 17, 2012), *available at* http://ftc.gov/os/caselist/1023172/121107plspaydaycmpt.pdf.

32. *Id.* ¶¶ 11–14.

33. *Id.* ¶¶ 15–19.

34. *Id.* ¶¶ 20–34.

In a stipulated final judgment and decision and order, the court imposed a civil penalty of $101,500.[35] PLS was also prohibited from further statutory violations of the FCRA and GLBA, ordered to implement an information security program, and required to obtain biennial assessments from a third-party professional.[36]

Compete, Inc.

FTC action against Compete, Inc. ("Compete") showed the agency's concern for notice in connection with the collection of personal information from consumers' web activities.[37] Compete is a market research firm that collected consumer information through its own software products, including a "Toolbar" that allowed consumers to access information about websites and a "Consumer Input Panel" that allowed consumers to win rewards after expressing their opinions.[38] It also licensed these software products to third parties, through which Compete also gathered data.[39] Compete disclosed some data collection in its privacy policies accompanying these software products, but failed to disclose the extent of its data collection, including its capture of information communicated on secure, third-party websites (such as credit card data, security codes, and Social Security numbers).[40] It also collected more than browsing behavior, including details such as whether a consumer made or abandoned a purchase of an item in an online shopping cart.[41] Despite its contrary representations, Compete also failed to strip all personal information from data collected before transmitting it from consumers' computers, and its filters failed to prevent the collection of sensitive data.[42] Compete's actions diverged from its statements to take reasonable security measures to protect consumer data, such as by transmitting information gathered in plain text.[43]

In its decision and order, the FTC prohibited Compete from collecting information unless (i) it has prominently and clearly displayed, separate from any privacy policy or similar document, the types of information that will be collected and how the information will be used, and (ii) it obtains affirmative consent from the consumer to the collection, use, or sharing of the information.[44] Compete was also prohibited from using the information gathered contrary to the standards set out in the order, unless consumers consent after appropriate

35. Stipulated Final Judgment and Order for Payment of Civil Penalties, Permanent Injunction, and Other Equitable Relief at 5, United States v. PLS Fin. Servs., Inc., Case No. 1:12-cv-8334 (N.D. Ill. Oct. 26, 2012), *available at* http://ftc.gov/os/caselist/1023172/121107plspaydaystip.pdf.

36. *See id*. at 6–10.

37. Complaint, *In re* Compete, Inc., No. 102-3155, 2013 WL 752477 (FTC Feb. 20, 2013).

38. *Id*. at *1.

39. *Id*.

40. *Id*. at *1–2.

41. *Id*. at *2.

42. *Id*. at *2–3.

43. *Id*. at *3–4.

44. *In re* Compete, Inc., No. 102-3155, 2013 WL 752477, at *11–19 (FTC Feb. 20, 2013) (decision and order).

notification.[45] The FTC required Compete to inform consumers how to permanently disable or uninstall its data collecting products, as well as to maintain a customer support e-mail address and phone line for these purposes.[46] Further, Compete must develop an information security program and submit to biennial assessments from a qualified third party.[47]

Equifax Information Services LLC and Direct Lending Source, Inc.

The FTC addressed the FCRA and transparency in its action against Equifax Information Services LLC ("Equifax").[48] In violation of the FCRA requirement to limit access to consumer reports only for a permissible purpose, Equifax sold "prescreened lists" of consumers late on mortgage payments to Direct Lending Source, Inc. or its affiliates (collectively, "Direct Lending"), which used these prescreened lists for general marketing, not to make a "firm offer of credit or insurance" as required by the FCRA.[49] Direct Lending also sold these lists to other marketers, many of which did not have a permissible purpose to receive them.[50] The FTC claimed Equifax failed to employ reasonable measures to control access to sensitive consumer financial information.[51] Among its alleged shortcomings, Equifax continued to sell prescreened lists to Direct Lending even though it knew those lists were being resold to others without a permissible purpose for obtaining them.[52] Moreover, Equifax provided those lists through an online portal, which was also utilized by third parties in connection with Direct Lending's operations.[53] The FTC claimed that Equifax failed to employ reasonable efforts to verify the identities of these third parties accessing information it controlled, and thus could not ensure that they were entitled to receive the information.[54]

In the decision and order, the FTC imposed a civil penalty of $392,803 and enjoined Equifax from furnishing prescreened lists in violation of the FCRA.[55] In a related action against Direct Lending, the court ordered a $1.2 million civil penalty, enjoined further use or furnishing of consumer reports in violation of the FCRA, and imposed additional remediation and compliance obligations.[56]

45. *Id.* at *13–14.
46. *Id.*
47. *Id.* at *16–17.
48. Complaint, *In re* Equifax Info. Servs. LLC, No. 102-3252, 2013 WL 1151916 (FTC Mar. 5, 2013).
49. *Id.* at *1–2.
50. *Id.* at *2.
51. *See id.*
52. *Id.*
53. *Id.*
54. *See id.*
55. *See In re* Equifax Info. Servs. LLC, No. 102-3252, 2013 WL 1151916, at *3–8 (FTC Mar. 5, 2013) (decision and order).
56. Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 6–14, United States v. Direct Lending Source, Inc., No. 3:12-cv-02441-DMS-BLM (S.D. Cal. Oct. 11, 2012), *available at* http://ftc.gov/os/caselist/1023000/121010directlendingstip.pdf.

DesignerWare, LLC and Rent-to-Own Computer Stores

The FTC brought an action against DesignerWare, LLC and certain of its corporate officers (collectively, "DesignerWare") based on notice and transparency concerns involving the collection of personal information.[57] DesignerWare licensed a software product to rent-to-own stores designed to help a lessor track and communicate with its rented computers.[58] DesignerWare recommended that its licensees disclose the presence of the software on a rented computer when a consumer signed a contract to rent, but it did not require this practice or otherwise ascertain whether its licensees followed that recommendation.[59] Through the software, licensees were able to collect personal information through key logging, geolocation tracking, and even taking pictures of computer users.[60] In its decision and order, the FTC prohibited DesignerWare from using monitoring technology to gather information from rented computers or from licensing the same for use on rental computers.[61] It also enjoined gathering data via geophysical location without providing clear and prominent notice at the time the computer is rented and immediately prior to each use of such technology and ensuring that the renter's affirmative, express consent is obtained when the computer is rented, including the use of a notice icon when location technology is activated.[62] Related actions against seven of DesignerWare's licensees resulted in similar restrictions on information gathering practices and enhanced disclosure requirements to customers.[63]

Google Inc.

Notice, choice, and transparency concerns animated further action against Google Inc. ("Google") for a violation of its previous consent order concerning the use of cookies without customer consent.[64] The FTC alleged that Google violated the previous consent order by placing cookies on users' computers without their knowledge, enabling targeted advertisements based upon those cookies, and thereby misrepresenting individuals' ability to control the collection of information and violating the previous consent decree's prohibition against such a misrepresentation.[65] In addition, Google allegedly misrepresented its compliance with the NAI Code by failing to disclose its information collection, and also violated the previous consent decree's prohibition against misrepresent-

57. Complaint, *In re* DesignerWare, LLC, No. 112-3151, 2013 WL 1684151 (FTC Apr. 11, 2013).
58. *Id.* at *1–2.
59. *Id.* at *2.
60. *Id.* at *2–4.
61. *In re* DesignerWare, LLC, No. 112-3151, 2013 WL 1684151, at *6–13 (FTC Apr. 11, 2013) (decision and order).
62. *Id.* at *8–10.
63. *See* Press Release, Fed. Trade Comm'n, FTC Approves Final Order Settling Charges Against Software and Rent-to-Own Companies Accused of Computer Spying (Apr. 15, 2013), *available at* http://ftc.gov/opa/2013/04/designerware.shtm.
64. *See* United States v. Google, Inc., No. CV 12-04177 SI, 2012 WL 5833994 (N.D. Cal. Nov. 16, 2012).
65. *Id.* at *1.

ing its adherence with such a code.[66] In a stipulated order, Google was ordered to pay a civil penalty of $22.5 million, to maintain systems that delete Google cookies from Safari browser users, and to report on its compliance.[67]

HireRight Solutions, Inc.

Notice, transparency, and accuracy concerns were also raised in an action against HireRight Solutions, Inc. ("HireRight").[68] HireRight was a "consumer reporting agency" under the FCRA, which sold background-screening reports to assist employers with employment decisions.[69] HireRight failed to follow reasonable procedures to ensure maximum possible accuracy of consumer reports, resulting in erroneous information that harmed consumers.[70] In violation of the FCRA, HireRight also allegedly failed to (i) provide consumers access to their reports and appropriate procedures to correct errors, (ii) promptly reinvestigate consumer claims about inaccuracy, and (iii) follow notice and accuracy procedures designed to ensure that public record information it provided was complete and current.[71] In a stipulated order, HireRight received a civil penalty of $2.6 million and was enjoined from further FCRA violations.[72]

EPN, Inc. and Franklin's Budget Car Sales, Inc.

In its actions against EPN, Inc. ("EPN") and Franklin's Budget Car Sales, Inc. ("Franklin's"), the FTC focused on data security concerns arising from peer-to-peer file sharing software installed on corporate computers that leaked consumer information to the public.[73] According to the FTC, this demonstrated a lack of reasonable and appropriate information security.[74] Both entities were enjoined from further violations and required to perform security assessments.[75]

66. *Id.*
67. *Id.* at *2–6.
68. Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief, United States v. HireRight Solutions, Inc., No. 1:12-cv-01313 (D.D.C. Aug. 8, 2012), *available at* http://www.ftc.gov/os/caselist/1023130/120808hirerightcmpt.pdf.
69. *Id.* ¶¶ 8–11.
70. *Id.* ¶¶ 12–14.
71. *Id.* ¶¶ 15–20.
72. Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 3–6, United States v. HireRight Solutions, Inc., No. 1:12-cv-01313 (D.D.C. Aug. 8, 2012), *available at* http://ftc.gov/os/caselist/1023130/120808hirerightstip.pdf.
73. Complaint, *In re* EPN, Inc., No. 112-3143, 2012 WL 5375158, at *1–2 (FTC Oct. 3, 2012); Complaint, *In re* Franklin's Budget Car Sales, Inc., No. 102-3094, 2012 WL 5375157, at *1–2 (FTC Oct. 3, 2012).
74. Complaint, *In re* EPN, Inc., No. 112-3143, 2012 WL 5375158, at *2 (FTC Oct. 3, 2012); Complaint, *In re* Franklin's Budget Car Sales, Inc., No. 102-3094, 2012 WL 5375157, at *2–4 (FTC Oct. 3, 2012).
75. *In re* EPN, Inc., No. 112-3143, 2012 WL 5375158, at *2–7 (FTC Oct. 3, 2012) (decision and order); *In re* Franklin's Budget Car Sales, Inc., No. 102-3094, 2012 WL 5375157, at *4–9 (FTC Oct. 3, 2012) (decision and order).

Wyndham Worldwide Corp.

Data security was also the focus of an action against Wyndham Worldwide Corp. and related entities (collectively, "Wyndham"). The FTC alleged that Wyndham engaged in a number of practices that, taken together, unreasonably and unnecessarily exposed and compromised consumers' personal data.[76] However, Wyndham claims that the FTC overstepped its authority by setting data security standards for companies.[77]

Warning Letters

In conjunction with an international privacy protection effort by the Global Privacy Enforcement Network, the FTC issued warning letters to ten data brokers regarding possible violations of the FCRA.[78] In a test-shopping operation, FTC staff members posed as others seeking information about consumers to make decisions about their creditworthiness, eligibility for insurance, or suitability for employment.[79] Of the forty-five companies contacted by FTC staffers, ten appeared to violate the FCRA by offering information without complying with the law.[80]

Revisions to COPPA

The FTC revised the COPPA Rule[81] to become more comprehensive.[82] Among other things, these amendments included the following changes: (i) clarifying that "personal information" includes geolocation information, photographs, and videos; (ii) offering a streamlined approval process for obtaining parental consent; (iii) clarifying obligations for apps and third parties; (iv) strengthening data security protections from covered websites and service providers; and (v) enhancing the FTC's oversight of self-regulatory safe harbor programs.[83]

76. Complaint for Injunctive and Other Equitable Relief, FTC v. Wyndham Worldwide Corp., No. 12CV01365, 2012 WL 2389423 (D. Ariz. June 26, 2012).

77. Brent Kendall, *Legal Showdown on Cybersecurity; Hotelier Wyndham Challenges FTC's Authority to Police Corporate Data Practices*, Wall St. J. (May 12, 2013, 8:51 PM), http://goo.gl/64if5A; Ed Beeson, *Unwanted Hotel Charges; Wyndham Claims FTC Overreach in Data Breach Lawsuit*, NJ.com Blog (June 2, 2013, 8:00 AM), http://www.nj.com/business/index.ssf/2013/06/hotel_charges_wyndham_chain_fi.html.

78. Press Release, Fed. Trade Comm'n, FTC Warns Data Broker Operations of Possible Privacy Violations (May 7, 2013), *available at* http://www.ftc.gov/opa/2013/05/databroker.shtm.

79. *Id.*

80. *Id.*

81. 16 C.F.R. § 312 (2013).

82. Press Release, Fed. Trade Comm'n, FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information by Amending Children's Online Privacy Protection Rule (Dec. 19, 2012), *available at* http://www.ftc.gov/opa/2012/12/coppa.shtm.

83. *Id.*; *see also* Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972 (Jan. 17, 2013) (to be codified at 16 C.F.R. pt. 312).

FTC Staff Reports

The FTC released two reports focused on mobile privacy, *Mobile Privacy Disclosures: Building Trust Through Transparency* ("Disclosure Report") and *Mobile Apps for Kids: Disclosures Still Not Making the Grade* ("Kids Report").[84] In the Disclosure Report, the FTC offered recommendations for best practices on mobile privacy disclosures.[85] In the Kids Report, the FTC followed up on its prior reported investigations concerning unauthorized information disclosures from various computer applications, determined that there was little or no improvement in disclosures made, and found a significant discrepancy between privacy disclosures and actual practices of surveyed apps.[86] Such discrepancies could constitute violations of COPPA or "unfair" or "deceptive" practices under the FTC Act.[87]

With the increased ability to recognize faces using widespread technology, the FTC also released a report on best practices surrounding facial recognition technology.[88]

Conclusion

Recent actions have continued to emphasize the need for companies to implement reasonable data security measures and provide notice, choice, and transparency to consumers. The FTC has also increased its attention to privacy for newer technologies, such as mobile and facial recognition, through workshops and reports. While the FTC has followed through on its commitment to address privacy protections, recent challenges to that authority raise new questions about who will serve as privacy sheriff, and may well trigger renewed attention to other means of privacy enforcement.

84. Fed. Trade Comm'n, Mobile Privacy Disclosures: Building Trust Through Transparency (2013) [hereinafter Mobile Privacy Disclosures], *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf; Fed. Trade Comm'n, Mobile Apps for Kids: Disclosures Still Not Making the Grade (2012) [hereinafter Mobile Apps for Kids], *available at* http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf.

85. Mobile Privacy Disclosures, *supra* note 84, at 13–27.

86. Mobile Apps for Kids, *supra* note 84, at 21.

87. *Id.*

88. Fed. Trade Comm'n, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies (2012), *available at* http://ftc.gov/os/2012/10/121022facialtechrpt.pdf.

Recent Developments in Mobile Privacy Law and Regulation

*By Robert V. Hale II**

Introduction

As the use of mobile devices continues to expand, both federal and state regulators have taken notice in the form of consumer privacy enforcement actions and guidance aimed at both device manufacturers and companies with mobile applications ("apps"), not to mention app developers and cloud service providers. Recent enforcement actions involving privacy violations have included the case of the Federal Trade Commission ("FTC") against mobile device manufacturer HTC America[1] and the California Attorney General's case against Delta Air Lines.[2] Additionally, both the FTC[3] and the California Attorney General's Office[4] have recently issued guidance specifically addressing privacy compliance for mobile devices and apps. The FTC has also released guidance on mobile-specific privacy disclosure practices.[5] These developments serve as a useful harbinger for assessing consumer privacy risks and mitigation strategies in this quickly evolving area of e-commerce. They also highlight the increasingly active role that the FTC and large states such as California have taken recently in light of the absence of any federal law imposing data security standards on all businesses in all industries.[6]

* Rob Hale serves as Corporate Counsel for Apollo Education Group, where his duties include transactional and regulatory matters. Prior to this, he held similar roles at HSBC and other financial institutions.

1. Press Release, Fed. Trade Comm'n, HTC America Settles FTC Charges It Failed to Secure Millions of Mobile Devices Shipped to Consumers (Feb. 22, 2013), *available at* http://www.ftc.gov/opa/2013/02/htc.shtm.

2. Press Release, Cal. Att'y Gen., Attorney General Kamala D. Harris Files Suit Against Delta Airlines for Failure to Comply with California Privacy Law (Dec. 6, 2012), *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-files-suit-against-delta-airlines-failure.

3. Fed. Trade Comm'n, Mobile App Developers: Start with Security (Feb. 2013) [hereinafter Mobile App Developers], *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

4. Cal. Att'y Gen., Privacy on the Go: Recommendations for the Mobile Ecosystem (Jan. 2013) [hereinafter Privacy on the Go], *available at* http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

5. Fed. Trade Comm'n, Mobile Privacy Disclosures: Building Trust Through Transparency (Feb. 2013), *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.

6. *See* Corey M. Dennis, *Data Security Laws and the Rising Cybersecurity Debate*, Lexology (Jan. 28, 2013), http://goo.gl/g7uv0L.

HTC America

In February 2013, the FTC brought charges against mobile device manufacturer HTC America ("HTC") alleging that the company failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers, introducing security flaws that placed sensitive information about millions of its consumers at risk.[7] In particular, HTC customized its Android-based operating system by preinstalling certain applications, and in doing so preempted a user's ability to receive notice of what sensitive information such applications would require and an option for the user to choose whether to install the application.[8] In settling these charges with HTC, the FTC's consent order not only requires HTC to establish a comprehensive security program, it also prohibits HTC from making any false or misleading statements about the security and privacy of consumers' data on HTC devices.[9]

Although it is not unusual for companies facing FTC scrutiny for privacy practices to settle by way of a consent order,[10] or otherwise, Wyndham Hotels and Resorts recently decided to challenge the FTC's authority to use its consumer protection law to regulate security practices at American companies absent specific legislation.[11] In response to FTC allegations that Wyndham failed to maintain adequate security measures to prevent security breaches that resulted in more than $10.6 million in fraudulent charges on consumers' accounts, Wyndham has asked a federal court to throw out the FTC's complaint on the ground that the FTC is holding Wyndham accountable for the actions of hackers, rather than pursuing the hackers themselves.[12] Wyndham also cites the lack of any security standards promulgated by the FTC and the lack of congressional action in the area of data security as further evidence of the FTC's overreaching.[13] The *Wyndham* case should be watched closely given that a decision in Wyndham's favor could have significant implications for the future efficacy of the FTC's enforcement authority in the area of data security.

FTC's New Privacy Guidance for Mobile App Developers

Announcement of the HTC settlement coincided with the FTC's release of a new business guide that encourages mobile app developers to aim for reasonable data security.[14] The guidance outlines key considerations for app developers in

7. Complaint ¶ 7, *In re* HTC Am., Inc., No. 122-3049, 2013 WL 752478, at *1 (FTC Feb. 22, 2013).

8. *Id.* ¶¶ 4–6, 2013 WL 752478, at *1.

9. Agreement Containing Consent Order ¶¶ 1–2, *In re* HTC Am., Inc., No. 122-3049, 2013 WL 752478, at *9 (FTC Feb. 22, 2013).

10. *See generally FTC Resources for Reporters*, FTC.GOV, http://www.ftc.gov/opa/reporter/privacy/privacypromises.shtml (last modified May 3, 2013). Companies that have settled privacy-related FTC enforcement actions over the last two years include Facebook, Google, Cbr Systems, Inc. (cord blood registry), RockYou (social game site), EPN, Inc. (debt collector), and Franklin's Budget Car Sales, Inc.

11. Brent Kendall, *Legal Tempest Over Cybersecurity*, WALL ST. J., May 13, 2013, at B10.

12. *Id.*

13. *Id.*

14. *See* MOBILE APP DEVELOPERS, *supra* note 3, at 1.

adopting and maintaining reasonable data security practices, all of which would be standard procedure (and common sense) for traditional software vendors, but could be overlooked in the "mobile ecosystem" due to the speed and relative ease with which mobile apps can be produced and released to the public.[15] The guidance provides twelve "tips" for mobile app security, which can be summarized as follows: (1) *Make someone responsible for security*—Don't assume someone else is handling it; (2) *Take stock of the data you collect and retain*—Don't collect or keep data you don't need; (3) *Understand differences between mobile platforms*—Do your research and adapt your code accordingly; (4) *Don't rely on a platform alone to protect your users*—Understand the limitations of platform security and take other measures necessary to protect users. (5) *Generate credentials securely*—Usernames and passwords must be appropriately secured. (6) *Use transit encryption for usernames, passwords, and other important data*—Given that mobile devices commonly rely on unsecured Wi-Fi access points, protect users by deploying in HTTPS or another industry standard protocol; (7) *Use due diligence on libraries and other third-party code*—Third-party source can contain security vulnerabilities and must be thoroughly vetted; (8) *Consider protecting data you store on a user's device*—Use encryption or special storage schemes to protect personal information from viruses, malware, or a lost/stolen device; (9) *Protect your servers, too*—Servers that communicate with apps must also be secured, including those deployed through commercial cloud providers where divisions of responsibility for security can often fall heavily on the app developer;[16] (10) *Don't store passwords in plaintext*—Verification functions should utilize the latest industry-standard protections, including encryption and hash values; (11) *You're not done once you release your app. Stay aware and communicate with your users*—Apps must be constantly monitored for security vulnerabilities and updates; and (12) *If you're dealing with financial data, health data, or kids' data, make sure you understand applicable standards and regulations*—The guidance provides links to additional resources concerning the applicable standard and regulations for these sensitive data subjects.[17] In reviewing privacy and security policies that cover mobile apps or devices, practitioners should ensure that their clients can validate any claims concerning the use of "reasonable" or "industry standard" security measures against this and other FTC guidance.

Delta Air Lines

In December 2012, California's Attorney General sued Delta Air Lines for violating § 17200 and the California Online Privacy Protection Act.[18] The suit alleged that despite collecting substantial personally identifiable information

15. *Id.*

16. *See* Amazon Web Servs., Overview of Security Processes 4 (Mar. 2013), *available at* http://awsmedia.s3.amazonaws.com/pdf/AWS_Security_Whitepaper.pdf ("[Y]ou assume responsibility and management of the guest operating system (including updates and security patches), other associated application software, as well as the configuration of the AWS-provided security group firewall.").

17. Mobile App Developers, *supra* note 3, at 2–5.

18. Complaint ¶ 4, California v. Delta Air Lines, Inc., No. CGC-12-526741 (Cal. Super. Ct. Dec. 6, 2012), *available at* http://oag.ca.gov/system/files/attachments/press_releases/Delta%20Complaint_0.pdf.

such as a user's full name, telephone number, e-mail address, frequent flyer account number and pin code, photographs, and geo-location, the company's Fly Delta application did not have a privacy policy to inform users of what personally identifiable information Delta collects about them, how Delta uses that information, or to whom that information is shared, disclosed, or sold.[19] According to the complaint, two months prior to filing the suit, the California Attorney General's office sent Delta a letter, notifying the company of its non-compliance and requesting a response within thirty days.[20] Although Delta acknowledged receipt of the letter to the press, it did not respond to the letter or otherwise demonstrate to the California Attorney General that it had posted a privacy policy for users of its Fly Delta app.[21]

On May 9, 2013, a California state court dismissed with prejudice the state's lawsuit against Delta. In sustaining Delta's demurrer to the complaint, although the court did not explain its reasoning in its two-page order, it appears the court agreed with Delta's argument that the California statute does not apply to airlines and is preempted by federal law.[22] Although it is unclear whether at this stage the California Attorney General will continue to pursue its case against Delta, apparent federal preemption of the case potentially limits state efforts to impose data security standards across industries, particularly those heavily regulated by federal law.

California Attorney General's *Joint Statement of Principles* and *Recommendations for Mobile Privacy*

Following the *Delta* suit, the State of California entered into a Joint Statement of Principles with Apple, Google, Microsoft, Amazon, Hewlett-Packard, and Research in Motion requiring all applications offered through the companies' mobile platforms to have privacy policies concerning any collection of personal information.[23] The Joint Statement also outlines several other related obligations, including implementation of a process for allowing users to report non-compliance.[24] Although the Joint Statement expressly provides that it is "not intended to impose legally binding obligations on the Participants or affect existing obligations under law [. . .],"[25] it also specifies that compliance with its provisions "will not limit law enforcement or any other regulator's right to pursue an action against a developer for alleged violation of applicable law."[26] As such, the Joint Statement is clearly intended to serve as an indicator to the entire mobile industry that the

19. *Id.*
20. *Id.* ¶ 22.
21. *Id.* ¶ 23.
22. *See* Katie W. Johnson, *California Court Dismisses State AG's Mobile App Privacy Lawsuit Against Delta*, Bloomberg BNA (May 21, 2013), http://www.bna.com/california-court-dismisses-n17179873953/.
23. Cal. Att'y Gen., Joint Statement of Principles (Feb. 2013), *available at* http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf.
24. *Id.* ¶ 6.
25. *Id.* ¶ 1.
26. *Id.* ¶ 6.

State of California takes privacy compliance seriously. As of October 2012, all the app store companies that joined the agreement reported that they had implemented the principles.[27]

Also following *Delta*, California's Attorney General released a set of guidelines outlining best practices to ensure privacy compliance and encourage mobile app developers and others to consider privacy practices in their initial design stages.[28] More detailed in its scope than the FTC's aforementioned Mobile App Developers guidance,[29] Privacy on the Go provides a process for app developers to follow, including a checklist of the types of data the app could potentially collect, use, and disclose, as follows:

- Unique device identifiers;
- Geolocation data, including data collected through GPS, WiFi, and user entry;
- Mobile telephone numbers;
- E-mail addresses;
- User names;
- Text messages or e-mails;
- Call logs;
- Contacts and address book entries;
- Financial or payment information;
- Health or medical information;
- Photos or videos;
- Internet browsing history; and
- Other apps downloaded or used.[30]

Developers should then take the following questions into consideration for each type of data:

- Is the data necessary for the basic functionality of the app?
- Is the data necessary for other business purposes, such as billing?
- How will the data be used?
- Is it necessary to store the data off the mobile device, on the app developer's servers?
- How long does the data need to be stored on the app developer's servers?

27. Privacy on the Go, *supra* note 4, at 4.
28. *Id.* at 1.
29. Mobile App Developers, *supra* note 3.
30. Privacy on the Go, *supra* note 4, at 8.

- Will the app developer share the data with third parties, such as advertising networks, analytics companies, or service providers?
- How will third parties use the data?
- Who within the app developer's organization will have access to user data?
- Is the app directed to or likely to be used by children under the age of thirteen?
- What parts of the mobile device does the app developer have permission to access?
- Can the app developer provide users with the ability to modify permissions?[31]

Privacy on the Go further recommends that in addition to providing users a general privacy policy before a mobile app is downloaded, app developers should also consider use of "special notices" that would alert users in advance to data practices that may be unrelated to an app's basic functionality or that involve sensitive information and offer users the opportunity to allow or prevent the practice.[32] The report also calls on advertising networks to establish greater control for mobile users over the use of personally identifiable information by third parties for behavioral advertising.[33] Lastly, the report urges collaboration between operating system developers and mobile carriers in patching security vulnerabilities and related privacy best practices.[34]

Conclusion

In a recent speech by FTC Commissioner Julie Brill delivered before the Direct Marketing Association, Commissioner Brill emphasized the FTC efforts to safeguard consumers' privacy online and in the mobile environment.[35] In doing so she characterized the FTC's efforts to protect consumer privacy as helpful to businesses by ensuring consumers do not abandon the mobile marketplace and continue to use apps that collect data benefitting the direct marketing industry.[36]

As the developments noted herein and Commissioner Brill's recent comments make clear, the growing ascendancy of mobile devices as the primary means through which consumers access the internet has not gone unnoticed by state and federal regulators. Companies' mobile business strategies, whether relating

31. *Id.*
32. *Id.* at 5.
33. *Id.* at 15.
34. *Id.* at 16.
35. Julie Brill, Comm'r, Keynote Third Annual Public Policy Institute on Financial Services Law and Economics Center, George Mason University (May 2, 2013), *available at* http://www.ftc.gov/speeches/brill/130502gmu-keynote.pdf.
36. *Id.* at 5.

to technology, e-commerce, marketing, or otherwise, will need to take data privacy compliance into account early on and remain focused on best practices based on guidance from state and federal authorities, including the FTC and the California Attorney General's office, not to mention an evolving body of case law concerning the application of existing statutory restrictions to mobile devices and apps.

Global Privacy and Data Security Developments—2013

*By Katherine Ritchey, Mauricio Paez, Veronica McGregor, and Maria Sendra**

Privacy and data security continue to be a focus for corporations, regulators, law enforcement, and consumer groups across the globe. Imaginative ways to access and use information create significant challenges in how we protect individuals, nations, and an interconnected world economy. These issues touch virtually every aspect of modern life, from the use of smart phones to global security against terrorism. This survey covers significant developments in global privacy and data security and topics to watch in the coming year.

Privacy in the Cloud

Cloud computing services challenge traditional privacy law concepts as well as regulators who struggle to keep up with technological developments. "Cloud" refers to a distributed internet-based infrastructure used on a shared basis[1] in which user data may be stored in different or multiple data centers around the world.

Jurisdiction and Access to Data

A key area of ongoing debate regarding the cloud is jurisdiction and territoriality, which are central to privacy regulation. The legal framework regulating data transfers lags behind cloud computing innovation,[2] and there is not agreement on a new legal framework. Generally, there are two bases for jurisdiction over the cloud: 1) location of the infrastructure (e.g., data centers) and 2) location of the providers.[3]

---

* The authors are partners at Jones Day who advise on a broad range of privacy and data security issues, including worldwide legal requirements regarding data protection, transfers and breaches, worldwide policies and compliance procedures for handling and safeguarding personal and company information, litigation, payments, and other issues.

The authors thank Emily Douglas, Louise Doyle, Eric Fleekop and Nandini Iyer for their assistance.

1. Peter Mell & Timothy Grance, The NIST Definition of Cloud Computing (Sept. 2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

2. Eur. Parliament Directorate-Gen. for Internal Policies, Study: Fighting Cyber Crime and Protecting Privacy in the Cloud (Oct. 2012), *available at* http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050.

3. *See id*. at 38.

The Patriot Act[4] and the Foreign Intelligence Surveillance Act[5] are examples in which provider-based jurisdiction potentially conflicts with infrastructure-based jurisdiction. U.S. companies may be required to disclose the cloud data of an EU citizen stored in an EU data center to the U.S. government under the Patriot Act.[6] The U.S. laws in this regard are not unique. For example, German law enforcement has tapped cloud data abroad using mutual law enforcement treaties.[7] EU finance regulations permit auditing of data in the cloud because it is considered outsourcing.[8] Expect continued activity as regulators struggle with jurisdiction in the cloud.

EU v. U.S. Approaches to the Cloud

As various regulators impose a privacy framework on the cloud, their differing approaches to privacy are fueling debate. Both the European Union and United States provided guidance regarding cloud data last year. Not surprisingly, they are not in agreement on the topic. In September 2012, the European Union issued an advisory communication[9] that calls for greater data protection in the cloud. By the end of 2013, the Commission expects to create model contract terms and a model code of conduct for cloud providers.[10]

The European Data Protection Supervisor ("EDPS") supports rethinking data protection in the cloud because, according to the EDPS, currently it is impossible for data controllers purchasing cloud computing services to comply with legal data protection requirements.[11] For example, data controllers are held accountable for compliance with EU privacy laws even though they may not know where or how their data is stored by the data processor (the cloud provider) in the cloud.[12] The EDPS suggests clearly defining a "transfer" of personal data in the cloud as well as other solutions as the European Union moves toward increased regulation of the cloud.[13]

4. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of the U.S.C.).

5. 50 U.S.C. §§ 1801–1811, 1821–1829, 1841–1846, 1861–1862, 1871 (2012).

6. Zack Whittaker, *Patriot Act Can "Obtain" Data in Europe, Researchers Say*, CBS News (Dec. 4, 2012, 3:59 PM), http://www.cbsnews.com/8301-205_162-57556674/patriot-act-can-obtain-data-in-europe-researchers-say.

7. Johanna Laas, *. . . and the Cloud Again: German Government's Response to Formal Inquiry*, Privacy Eur. Blog (Apr. 29, 2013, 9:31 AM), http://www.privacy-europe.com/blog/and-the-cloud-again-german-governments-response-to-formal-inquiry/.

8. Lokke Moerel, Global Cloud Contracts: How to Navigate the EU Requirements in a Global Contract 4–5 (IAPP Global Privacy Summit, Mar. 6–8, 2013), *available at* https://www.privacyassociation.org/media/presentations/13Summit/S13_Closing_the_Deal_PPT.pdf.

9. *Communication from the Commission, Unleashing the Potential of Cloud Computing in Europe*, at 8, COM (2012) 529 final (Sept. 27, 2012).

10. *Id.* at 12–13.

11. *Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the Potential of Cloud Computing in Europe"* ¶ 25 (Nov. 16, 2012), *available at* http://goo.gl/FG9Dz.

12. *See id.* ¶ 24, 82.

13. *Id.* ¶ 74.

The International Trade Authority of the U.S. Department of Commerce ("ITA") has downplayed these concerns. Currently, U.S. privacy protection does not meet EU "adequacy" requirements, so moving data to the United States generally is not permitted unless the U.S. importer has certified to Safe Harbor Principles or entered an approved EU standard contract clause with the EU data exporter.[14] The ITA stated that it "does not believe that 'cloud computing' represents an entirely new business model or presents any unique issues for Safe Harbor."[15] This type of debate will continue as regulators struggle to address the cloud and other new technology.

Mobile Privacy

Mobile applications and "bring your own device" issues were significant in global mobile privacy debates in the last year.

Mobile Applications

Increased use of mobile devices and applications in lieu of personal computers is fueling privacy concerns. Mobile industry trade groups are encouraging self-regulation in an effort to limit government regulation.[16] Likewise, the PCI Security Standards Council released proactive Mobile Payment Acceptance Security Guidelines in September 2012, which provide global guidelines for payment applications operating on consumer mobile devices.[17]

In the United States, California Attorney General Kamala Harris continues to take a leadership role in the debate: After giving notice of her privacy concerns to popular mobile application operators, in December 2012, the California Attorney General filed a legal action alleging privacy deficiencies with a mobile application.[18] In January 2013, the California Attorney General also released a set of privacy best practice recommendations, including using clear and conspicuous privacy policies and limiting the personally identifiable information collected.[19]

14. U.S. Dep't of Commerce, Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing 1–2 (Apr. 12, 2013), *available at* http://goo.gl/IwqY2p.

15. *Id.* at 1.

16. *See, e.g.*, *A Status Update on the Development of Voluntary Do-Not-Track Standards: Before the S. Comm. on Commerce, Sci. & Transp.*, 113th Cong. (2013) (statement of Luigi Mastria, Managing Dir., Digital Advertising Alliance).

17. PCI Sec. Standards Council, PCI Mobile Payment Acceptance Guidelines for Developers (Sept. 2012), *available at* https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Developers_v1.pdf.

18. Press Release, Cal. Attorney Gen., Attorney General Kamala D. Harris Files Suit Against Delta Airlines for Failure to Comply with California Privacy Law (Dec. 6, 2012), *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-files-suit-against-delta-airlines-failure. The Delta suit was dismissed based on Airline Deregulation Act preemption. Karen Gullo, *Delta Wins Dismissal of California App Privacy Lawsuit*, Bloomberg.com (May 9, 2013, 1:36 PM CST), http://www.bloomberg.com/news/2013-05-09/delta-wins-dismissal-of-california-app-privacy-lawsuit.html.

19. Cal. Dep't of Justice, Privacy on the Go: Recommendations for the Mobile Ecosystem (Jan. 2013), *available at* http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

These actions are being watched closely by other law enforcement bodies and likely will be replicated elsewhere.

The Federal Trade Commission ("FTC") also has been active. In 2012, it announced best practices to protect consumers' private information by focusing on privacy during product development and more choice and transparency.[20] The FTC's enforcement activity likewise reflects its broadening approach to privacy. For example, in *In re HTC America, Inc.*, the FTC alleged that HTC, an upstream device and software provider with limited consumer interface, engaged in unfair and deceptive business practices in the customization of software used in certain mobile devices running third-party operating systems.[21]

Abroad, the European Union asserted that mobile applications are subject to the EU's Privacy and Electronic Communications Regulations, which require that users be informed about cookies and consent to their use.[22] A February 2013 Working Party Opinion clarified that processing personal data in mobile applications requires mobile application controllers to notify users of their rights of access, rectification, and erasure, along with their right to object to data processing.[23]

Bring Your Own Device ("BYOD")

Having employees use their personal devices for company business is an attractive option for employers because of the potential for reduced IT expenses and increased productivity. However, BYOD programs also implicate personal privacy and company security issues, including control of company information stored on employee-owned devices.[24] Solutions to protect confidential company data if a device is lost, such as "remote wipes," may also impact personal data, leading to potential liability for unauthorized access to the device under state and federal computer trespass laws.[25]

This issue is attracting increasing attention around the world. For example, in August 2012, the White House introduced a toolkit to support federal agencies

20. Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers (Mar. 2012), *available at* www.ftc.gov/os/2012/03/120326privacyreport.pdf.

21. *In re* HTC Am., Inc., No. 122-3049, 2013 WL 752478 (FTC Feb. 22, 2013) (proposing Agreement Containing Consent Order); *see also* Katherine S. Ritchey et al., *Lessons from* In re HTC America Inc.: *FTC's Broadening Approach to Consumer Data Security Leaves Unwary Manufacturer or Developer with More than It Bargained for*, Jones Day Publ'ns (Mar. 2013), http://www.jonesday.com/lessons_from_htc_america/.

22. Graeme Burton, *Android and iOS Apps Subject to EU Privacy Regulations—ICO*, Computing (May 18, 2012), http://www.computing.co.uk/ctg/news/2175933/android-ios-apps-subject-eu-privacy-regulations-ico.

23. *Opinion of the Article 29 Data Prot. Working Party on the 'Apps on Smart Devices'*, 00461/13/EN, WP 202 (Feb. 27, 2013), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

24. Philip Berkowitz, *Legal Challenges to 'Bring Your Own Device' Policies*, N.Y. L.J., July 12, 2012.

25. Charles Doyle, Cong. Research Serv., Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws (Dec. 27, 2010), *available at* http://www.fas.org/sgp/crs/misc/RS20830.pdf.

implementing BYOD programs.[26] In February 2013, the German Federal Office for Information Security provided recommendations on security strategy for BYOD programs.[27] Guidance from the United Kingdom's Information Commissioner's Office stresses that the data controller has the ultimate responsibility for ensuring legal compliance.[28] Expect new BYOD disputes and regulatory activity.

Global Developments in Addressing Cybersecurity Threats

Cyber-attacks around the globe commonly are headline news. They occur for many reasons, are perpetrated by different actors, and have diverse targets. Regulators are responding to protect regional and national interests, as well as the companies that operate in the overlapping universe of cyberspace.

On February 7, 2013, the European Parliament and the Council of the European Union adopted the *Directive Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union*.[29] The Directive provides that Member States shall ensure that public bodies, as well as operators of critical infrastructure, manage risks posed to the security of networks and information systems they control and use.[30] It also provides that Member States shall ensure the same entities report incidents of security breaches to proper authorities.[31]

After a series of failed legislation,[32] on February 12, 2013, President Obama issued an Executive Order titled Improving Critical Infrastructure Cybersecurity.[33] It directs the Secretary of Homeland Security to establish a "voluntary program" to support the adoption of a Cybersecurity Framework by owners and operators of critical infrastructure and other interested parties.[34] That same day, the Cyber Intelligence Sharing and Protection Act was re-introduced in Congress and later passed in the House.[35] A week later, the Obama Administration issued its Administration Strategy on Mitigating the Theft of U.S. Trade Secrets.[36] Each

26. Digital Servs. Advisory Grp. & Fed. Chief Info. Officers Council, Bring Your Own Device: A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs (Aug. 23, 2012), *available at* http://www.whitehouse.gov/digitalgov/bring-your-own-device.

27. German Fed. Office for Info. Sec., General Overview on Consumerisation and BYOD (Jan. 28, 2013), *available at* http://goo.gl/fF4WOX.

28. Info. Commissioner's Office, Data Protection Act 1998: Bring Your Own Device (BYOD) (2013), *available at* http://goo.gl/Eu1qML.

29. COM (2013) 48 final (Feb. 7, 2013), *available at* http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

30. *Id.* at 2.

31. *Id.*

32. *See, e.g.*, Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011 (PRECISE Act), H.R. 3674, 112th Cong. (2011); Cyber Intelligence Sharing and Protection Act (CISPA), H.R. 3523, 112th Cong. (2011); Cybersecurity Act of 2012, S. 2105, 112th Cong.

33. Executive Order No. 13636, 78 Fed. Reg. 11739 (Feb. 12, 2013).

34. *Id.* at 11741–42.

35. Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013).

36. Exec. Office of the President of the U.S., Administration Strategy on Mitigating the Theft of U.S. Trade Secrets (Feb. 2013), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

of these actions recognizes that U.S. companies are the target of sophisticated cyber-attacks that threaten U.S. economic interests and security.

At the 12th ASEAN Telecommunications and Information Technology Ministers Meeting in November 2012, the ministers of ten Asian countries reviewed progress in implementing ASEAN's Information and Communications Technology Master Plan, which incorporates a campaign to promote cybersecurity and collaboration with private industry, and reconfirmed formal collaboration strategies with Japan and South Korea on cybersecurity.[37]

These recent actions are not isolated; local, national, and regional governments are grappling with complicated issues presented by cyber-attacks, and how to coordinate with private industry and other governments. Critical infrastructure (including financial services, utilities, internet, transportation, and health care) is at risk, and protecting that infrastructure is a primary focus for many countries. Economic espionage and the theft of trade secrets also raise significant concerns for governments and the private sector.

Despite the widespread action around the globe in the last year, cybersecurity regulation is in its infancy. There is a robust debate on technical and practical issues relating to cybersecurity, and regulators are adopting varying—and potentially conflicting—approaches.

Global Data Breach Developments

Compromises of personal data have become commonplace; however, data breaches no longer are limited by geographic boundaries. The international trend toward establishing breach notification requirements continues, reflecting the expectation that notification enhances data security.

Both the United States and the European Union currently have a patchwork of data breach notification requirements. For example, in the United States, individual states differ on triggering events that require notification—"acquisition" of or "access" to personal information suffices in some states, while others require notification only after a risk-of-harm determination.[38] States also differ on when notification should be provided and to whom.[39] European nations have similar variations. For example, some nations require notifications to au-

37. Press Release, Ass'n of Se. Asian Nations, Joint Media Statement of the 12th ASEAN Telecommunications and IT Ministers Meeting and Its Related Meetings with Dialogue Partner (Nov. 19, 2012), *available at* http://www.asean.org/news/asean-statement-communiques/item/joint-media-statement-of-the-12th-asean-telecommunications-and-it-ministers-meeting-and-its-related-meetings-with-dialogue-partners.

38. *Compare* Haw. Rev. Stat. § 487N-1 (West, Westlaw through 2013 Act 228), *and* Me. Rev. Stat. Ann. tit. 10, § 1347(1) (West, Westlaw through 126th Legis. Sess.), *with* Alaska Stat. Ann. § 45.48.010(c) (West, Westlaw through 28th Legis. Sess.), *and* R.I. Gen. Laws. Ann. § 11-49.2-4 (West, Westlaw through 2013 Ch. 534).

39. *See, e.g.*, Wis. Stat. Ann. § 134.98(3) (West, Westlaw through 2013 Act 45); Vt. Stat. Ann. tit. 9, § 2430(a)–(d) (West, Westlaw through 2013 Sess.); *see also* Cal. Civ. Code §§ 1798.29; 1798.82(f) (West, Westlaw through 2013 Sess.) (providing that notification to the State Attorney General is required in some cases).

thorities and affected individuals, but others do not have mandatory notification to either the individuals or authorities.[40]

A more unified approach to data breach notification may be developing. The European Commission released a proposed General Data Protection Regulation[41] in 2012 that addresses data breach notification requirements throughout the European Union. The proposal is expected to be finalized in 2014, although likely will be amended from its current form. Similarly, in June 2012, the Data Security and Breach Notification Act of 2012 was introduced in the U.S. Senate to create a uniform federal privacy breach notification law to preempt the current patchwork of state laws.[42] This bill was reintroduced in the U.S. Senate on June 20, 2013, as the Data Security and Breach Notification Act of 2013.[43]

Authorities elsewhere in the world also are enacting breach notification laws, reflecting increased vigilance over data protection. For example, in August 2012, the Philippines passed its first consolidated data privacy legislation—the Data Privacy Act of 2012—influenced significantly by the European Union's current data protection laws.[44] South Korea's Personal Information Protection Act, effective in April 2012, mandates notification to individuals affected by a breach, as well as to the Korean government for large-scale breaches.[45] In April 2013, Australia introduced for the first time legislation regarding notification requirements for a "serious breach."[46]

Significant Global Privacy Developments

European Union

The European Union continues to forge an aggressive path in data privacy regulation, which likely will be followed in other parts of the world. The proposed General Data Protection Regulation ("Regulation")[47] sought to address legal uncertainty caused by inconsistent implementation of the 1995 Data Protection

40. *See, e.g.*, Bundesdatenschutzgesetz [Federal Data Protection Act], Dec. 20, 1990, as amended (Ger.) (noting that notification must be provided to both individuals and data protection authorities); Ley Orgánica de Protección de Datos de Carácter Personal [Organic Law of Personal Data Protection] (B.O.E. 2008, 298) (Spain) (providing general data protection guidelines, but not mandating notification to either affected individuals or authorities).

41. *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 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.

42. Data Security and Breach Notification Act of 2012, S. 3333, 112th Cong.

43. S. 1193, 113th Cong. (2013).

44. An Act Protecting Individual Personal Information and Communications Systems in the Government and the Private Sector, Rep. Act No. 10173 (Aug. 15, 2012) (Phil.), *available at* http://www.gov.ph/2012/08/15/republic-act-no-10173/.

45. Graham Greenleaf, *Major Changes in Asia Pacific Data Privacy Laws: 2011 Survey*, Privacy L. & Bus. Int'l Rep., Oct. 2011, at 5.

46. Jeremy Kirk, *Government Mulls Data Breach Notification Law, but Details Are Secret*, PC World Austl. (May 2, 2013, 5:46 AM), http://www.pcworld.idg.com.au/article/460753/goverment_mulls_data_breach_notification_law_details_secret/.

47. *See supra* note 41.

Directive by Member States and respond to advancements in technology. Among other reforms, the Regulation requires data controllers to appoint data protection officers, tightens consent rules, creates new rights for data subjects, augments data breach notification requirements, and strengthens noncompliance sanctions.[48] Various stakeholders within and outside Europe have weighed in on the Regulation, and the basis for much of the recent debate has been proposed amendments to the Regulation in the January 2013 draft report issued by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs ("LIBE"), the lead legislative committee for the Regulation.[49] Critics charge that LIBE's proposals generally increase burdens on data controllers, though others suggest that the more precise, technical language proposed by LIBE may be beneficial.[50] On October 21, 2013, LIBE adopted a version of the Regulation incorporating the Committee's proposals[51]; however, the text of the Regulation is by no means final. The European Parliament and Council of the European Union must now negotiate on the final version of the Regulation and will aim to reach agreement on this legislative reform before the May 2014 European elections.[52] Among the issues to watch are the scope of the regulation, the role of consent, restrictions on and accessibility to data, rules regarding international data transfers, and enforcement and remedies.

Hong Kong

In 2012, the Personal Data (Privacy) (Amendment) Ordinance[53] ("Amendments") was enacted to, among other things, strengthen restrictions on the use of personal data for direct marketing purposes. The Amendments, effective April 1, 2013, modify Hong Kong's 1997 Personal Data (Privacy) Ordinance ("PDPO")[54] by limiting companies' ability to engage in direct marketing without opt-in consent, which is enforced with criminal sanctions.[55] Despite a grandfathering provision, confusion and uncertainty persist on the use of personal data for direct marketing under the Amendments.[56] The Amendments also (i) gener-

48. *See supra* note 41.

49. Draft Report of the Committee on Civil Liberties, Justice and Home Affairs on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individual with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (Jan. 16, 2013), *available at* http://goo.gl/ycuwsN.

50. Allison Grande, *Changes in EU Data Protection Regime Could Repel US Cos.*, Law360 (Jan. 9, 2013, 11:21 PM), http://www.law360.com/articles/405883/changes-in-eu-data-protection-regime-could-repel-us-cos-.

51. Press Release, Eur. Parliament, Civil Liberties MEPs Pave the Way for Stronger Data Protection in the EU (Oct. 21, 2013), *available at* http://goo.gl/C707Mg.

52. *Id.*

53. Personal Data (Privacy) (Amendment) Ordinance, Ord. No. 18, (2012) (H.K.), *available at* www.gld.gov.hk/egazette/pdf/20121627/es12012162718.pdf.

54. Personal Data (Privacy) Ordinance, (2013) Cap. 486 (H.K.).

55. Office of the Privacy Comm'r for Personal Data, H.K., An Overview of the Major Provisions of the Personal Data (Privacy) (Amendment) Ordinance 2012 (2012), *available at* http://www.pcpd.org.hk/english/publications/files/ordinance2012_overview_e.pdf.

56. Anita Leung & Mauricio F. Paez, *Hong Kong Strengthens Its Personal Data Privacy Laws and Imposes Criminal Penalties on Direct Marketing*, Jones Day Publ'ns (May 2013), http://www.jonesday.com/

ally prohibit the disclosure of personal data without the consent of the individual from whom such data was collected ("Data Subject"), (ii) increase the Privacy Commissioner's enforcement powers under the PDPO, (iii) grant greater data access rights to Data Subjects, (iv) further regulate processing of personal data in outsourcing, and (v) include new exemptions to allow the use, disclosure, and/or transfer of personal data in specified circumstances.[57] The Amendments also permit legal assistance with claims made under the PDPO, criminalize disclosure of personal data for commercial gain and without consent, and impose certain restrictions and obligations concerning the outsourcing of data processing to third parties, some of which were put into operation in October 2012.[58]

Latin America

Latin American countries have been active in enacting privacy and data protection requirements. For example, on March 22, 2013, Peru issued implementing regulations for its 2011 data protection law,[59] which included new rules concerning the law's territorial scope, restrictions on data transfers, rights of data subjects in connection with notice and consent, and enforcement. Costa Rica also recently published regulations[60] to clarify its data protection law, which require expanded data breach notice, new registration obligations for data controllers, restrictions on personal data retention, express consent by a data subject for data processing, and direct compliance liability for data processors.[61]

On October 17, 2012, Colombia passed a comprehensive data protection framework to require, among other things, data subject notice and consent for personal data processing, restrictions on the processing of personal data of children, new rights of access and correction for data subjects, direct regulatory compliance obligations on service providers, international transfer restrictions, and data controller registration requirements.[62] Enforcement is entrusted in a new data protection authority, delegated under the Superintendency of Industry and Commerce.

What to Expect

Privacy and data security issues such as those highlighted in this survey, as well as others, will continue to develop around the world for the foreseeable

hong-kong-strengthens-its-personal-data-privacy-laws-and-imposes-criminal-penalties-on-direct-marketing-05-15-2013/.

57. *See id.*

58. *See id.*

59. Reglamento de la Ley No. 29733, Ley de Protección de Datos Personales del 22 de marzo del 2013 (Peru), *available at* http://spij.minjus.gob.pe/normas/textos/220313T.pdf.

60. Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, No. 37554-JP del 5 de marzo del 2013, *available at* http://www.tse.go.cr/pdf/normativa/reglamentoleyproteccionpersona.pdf.

61. Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, No. 8968 del 7 de julio del 2011 (Costa Rica), available *at* http://goo.gl/Ltmptp.

62. L. 1581, 17 de octubre del 2012, Diario Oficial [D.O.] (Colom.).

future. Technological advances create opportunities to access and use data in ways that were unimaginable even a few years ago, as well as risks to individuals, companies, and countries. Varying ideological approaches to privacy and data security in our interconnected digital world complicate the already difficult task of balancing innovation with reasonable protections. We are far from a mature global framework regulating privacy and data security, which means that uncertainty and change will be the norm in this space for years to come.

Electronically Stored Information in Litigation

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

I. Introduction

Recent developments in the use of electronically stored information ("ESI") in litigation center on two emerging themes: one technological—the increasing prominence of predictive coding; and one legal—the increasing stress on proportionality as a way to limit the burden and expense of discovery. The overriding question is no longer whether electronic discovery is necessary, but how to conduct it most effectively in terms of scope and cost. Courts and litigants are focusing on tools to harmonize the requirements imposed by case law and procedural rules with the equally binding laws of economics.[1]

II. Teaching Computers to Be Smarter than We Are: Predictive Coding

A. Emerging Case Law Supports Predictive Coding but Does Not Mandate It

The current buzz phrase in electronic discovery is "predictive coding." A 2012 case, *Da Silva Moore v. Publicis Groupe*,[2] first brought wide attention to predictive coding, inspiring articles like *Why Hire a Lawyer? Computers Are Cheaper*.[3] *Da Silva Moore* was a gender discrimination case against an advertising conglomerate in which the parties agreed to a protocol that called for the use of predictive coding, but plaintiffs later changed their minds.[4] Magistrate Judge Peck encouraged the use of predictive coding, which uses sample e-mail data to train software to identify relevant documents, explaining that "every person who uses email uses

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

1. For summaries of prior developments, see Timothy J. Chorvat & Laura E. Pelanek, *Electronically Stored Information in Litigation*, 68 Bus. Law. 245 (2012) (surveying developments in 2011–2012, focusing on discovery of social media and cloud data); Timothy J. Chorvat & Laura E. Pelanek, *Electronically Stored Information in Litigation*, 67 Bus. Law. 285 (2011) (surveying developments in 2010–2011, focusing on state courts); Timothy J. Chorvat & Laura E. Pelanek, *Electronically Stored Information in Litigation*, 66 Bus. Law. 183 (2010) (surveying developments in 2009–2010, focusing on federal courts).

2. 287 F.R.D. 182 (S.D.N.Y. 2012).

3. Joe Palazzolo, *Why Hire a Lawyer? Computers Are Cheaper*, Wall St. J. (June 18, 2012), http://online.wsj.com/article/SB10001424052702303379204577472633591769336.html.

4. *Da Silva Moore*, 287 F.R.D. at 183, 186–88.

predictive coding, even if they do not realize it. The 'spam filter' is an example of predictive coding."[5]

After the parties submitted the protocol and the court approved it,[6] plaintiffs challenged the protocol in several respects. Plaintiffs asserted that predictive coding "provides unlawful 'cover'" for defendant's counsel to escape their duty to certify that production is complete and correct under Rule 26(g) of the Federal Rules of Civil Procedure.[7] 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 that its production is 'complete'—but more importantly, Rule 26(g)(1) does not require that."[8] Plaintiffs also objected to the ESI protocol on the basis that it lacked a standard to determine whether the method is reliable.[9] Judge Peck described that objection as premature.[10]

Judge Peck observed that his opinion appeared to be the first to endorse the use of predictive coding, but he stressed that he was neither mandating predictive coding nor suggesting that predictive coding should be used in all cases.[11] Rather, "[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."[12]

Following *Da Silva Moore*, a Virginia state court ordered the use of predictive coding in *Global Aerospace, Inc. v. Landow Aviation, L.P.*[13] There, defendants sought approval to use predictive coding for the purposes of production.[14] The court granted that motion, but noted that the order was "without prejudice to a receiving party raising with the court an issue as to the completeness or the contents of the production or the ongoing use of predictive coding."[15]

In *National Day Laborer Organizing Network v. U.S. Immigration & Customs Enforcement Agency*,[16] Judge Scheindlin resolved disputes about the production of metadata and also addressed predictive coding. Plaintiffs brought that action seeking records from five federal agencies under the Freedom of Information Act.[17] The parties disputed the adequacy of the agencies' searches for responsive information.[18] Judge Scheindlin explained that "[i]t is impossible to evaluate the adequacy of an electronic search for records without knowing what search terms have

5. *Id.* at 184 n.2.
6. *Id.* at 187 & n.6 (noting an objection by plaintiffs).
7. *Id.* at 188 (citation omitted).
8. *Id.*
9. *Id.* at 189.
10. *Id.*
11. *Id.* at 193.
12. *Id.*
13. No. CL 61040, 2012 Va. Cir. LEXIS 50, at *2 (Apr. 23, 2012).
14. *Id.* at *1–2.
15. *Id.* at *2.
16. 877 F. Supp. 2d 87 (S.D.N.Y. 2012).
17. *Id.* at 93–94.
18. *Id.* at 94.

been used."[19] The court stressed that "[s]eemingly minor decisions—whether intentional or not—will have major consequences."[20] The court directed the parties to design new, targeted searches to address the deficiencies she noted and to provide full documentation of those searches, including custodians, sources, keywords, and Boolean search terms.[21] The court then recommended the use of predictive coding: "Through iterative learning, these methods (known as 'computer-assisted' or 'predictive' coding) allow humans to teach computers what documents are and are not responsive to a particular FOIA or discovery request and they can significantly increase the effectiveness and efficiency of searches."[22] The court suggested that, "if [the parties] wish to and are able to, then they may agree on predictive coding techniques and other more innovative ways to search."[23]

Vice Chancellor Laster of the Delaware Court of Chancery also issued a ruling supporting the use of predictive coding.[24] After deciding a motion for partial summary judgment in *EORHB Inc. v. HOA Holdings LLC*, he stated that "[t]his seems . . . to be an ideal non-expedited case in which the parties would benefit from using predictive coding."[25] Should the parties disagree with that assessment, Vice Chancellor Laster directed them to "show cause why this is not a case where predictive coding is the way to go."[26]

Another sign of the acceptance of predictive coding came in *Gabriel Technologies Corp. v. Qualcomm Inc.*,[27] where prevailing defendants sought attorney's fees with regard to plaintiffs' patent and trade secret claims.[28] The court awarded more than $12 million in fees,[29] including more than $2.8 million "for fees associated with a document review algorithm generated by [an] outside vendor."[30] In the motion seeking those fees, defendants explained that they had "collected almost 12,000,000 records—mostly in the form of . . . ESI . . . . Rather than manually reviewing the huge volume of resultant records, Defendants paid [a vendor] to employ its proprietary technology to sort these records into responsive and non-responsive documents."[31] The court found the "decision to undertake a more efficient and less time-consuming method of document review to be reasonable under the circumstances."[32]

19. *Id.* at 106.
20. *Id.* at 107.
21. *Id.* at 111.
22. *Id.* at 109.
23. *Id.* at 111.
24. Transcript of Oral Argument, EORHB Inc. v. HOA Holdings LLC, No. 7409-VCL (Del. Ch. Oct. 19, 2012) (order partially granting summary judgment for defendants and denying motion to dismiss counterclaims).
25. *Id.* at 66.
26. *Id.*
27. No. 08cv1992 AJB (MDD), 2013 U.S. Dist. LEXIS 14105 (S.D. Cal. Feb. 1, 2013).
28. *Id.* at *6–7.
29. *Id.* at *46.
30. *Id.* at *32.
31. *Id.* at *34–35 (citation and quotations omitted).
32. *Id.* at *35; *see also In re* Actos (Pioglitazone) Prods. Liab. Litig., No. 6:11-md-2299, 2012 U.S. Dist. LEXIS 187519, at *21, *25–26 (W.D. La. July 27, 2012) (approving protocol calling for predictive coding and specifying procedures).

On the other hand, Judge Miller applied considerations of proportionality to reject a request to direct a party solely to use predictive coding in *In re Biomet M2a Magnum Hip Implant Products Liability Litigation*.[33] There, defendant collected 19.5 million documents and used keywords and de-duplication to reduce the universe of potentially responsive materials to 2.5 million documents.[34] Biomet then used predictive coding to identify documents to be produced.[35] Plaintiffs contended that the use of keywords tainted the process and resulted in a reduced responsiveness rate.[36] Plaintiffs wanted defendant to apply predictive coding to the full universe of documents, but defendant objected on the basis of cost, noting that it spent more than $1 million on the initial production, and asserting that starting over would cost millions more.[37] The court noted that the issue was not "whether predictive coding is a better way of doing things than keyword searching prior to predictive coding," but "whether Biomet's procedure satisfies its discovery obligations."[38] The court found that Biomet's procedure fully complied with Rules 26(b) and 34(b)(2), as well as the Seventh Circuit Pilot Program's Principles Relating to the Discovery of Electronically Stored Information.[39] The court also rejected plaintiffs' request under the proportionality standard of Rule 26(b)(2)(C), based on its seven-figure cost.[40]

Magistrate Judge Nolan stressed the importance of cooperation while addressing a motion to compel the use of predictive coding in *Kleen Products LLC v. Packaging Corp. of America*.[41] There, plaintiffs complained about the defendants' use of a Boolean search method to identify responsive materials, arguing that the search was "subject to the inadequacies and flaws inherent when keywords are used to identify responsive documents."[42] Instead, plaintiffs requested the use of content-based advanced analytics to conduct natural language searches and subject matter searches.[43] Through two full days of evidentiary hearings related to ESI disputes, eleven status hearings, and three Rule 16 conferences, the parties resolved numerous issues, including search methodology.[44] Judge Nolan observed that Sedona Principle 6 states that "[r]esponding parties are best situated to evaluate the procedures, methodologies, and techniques appropriate for preserving and producing their own electronically stored information."[45] Ultimately, plaintiffs withdrew their request for predictive coding as to the document requests at issue, and they agreed to confer about appropriate search methodology for newly collected documents.[46]

33. No. 3:12-MD-2391 (N.D. Ind. Apr. 18, 2013) (order regarding discovery of ESI).
34. *Id.* at 2.
35. *Id.* at 2–3.
36. *Id.* at 3.
37. *Id.* at 3–4.
38. *Id.* at 4.
39. *Id.*
40. *Id.* at 5–6.
41. No. 10 C 5711, 2012 U.S. Dist. LEXIS 139632 (N.D. Ill. Sept. 28, 2012).
42. *Id.* at *14 (citation and quotations omitted).
43. *Id.* at *14–15.
44. *Id.* at *16–17.
45. *Id.* at *18 (citation and quotations omitted).
46. *Id.* at *19–20, *62–64.

B. The Predictive Coding Process

Courts seem favorably disposed toward predictive coding, but what is it? As a machine-learning technology, predictive coding requires litigants to take steps to "teach" the computer what documents are responsive.[47] The first step is to define the universe of materials to be reviewed, based on date range, file type, custodian, domain, or other parameters, excluding ranges known to be non-responsive.[48] Privileged documents also can be removed at the outset to avoid inadvertent production.[49] The next step is to estimate the yield of responsive documents from the collection by selecting and manually reviewing a statistically valid random sample from the universe.[50] If the yield of responsive documents is low, then the size of the control set may need to be adjusted.[51] The size of the control set is important because a poorly sized control set can affect the software's performance, and the results may not be reliable.[52]

With a control set in place, it is time to teach the computer. A training set of documents is selected, reviewed, and coded to train the software.[53] Generally, the documents in the training set are not chosen randomly; rather, responsive documents, together with some non-responsive documents, are selected for the training set using keywords or concept-based searches.[54] Based on the training set, the software creates a model that assigns a prediction score to each document based on degree of responsiveness.[55] The model is then tested, using the control set.[56] The software's predictions about responsiveness are compared to the coding decisions made by humans on the same set of documents.[57] If the desired performance metrics are not met, additional training sets are selected, trained, and tested.[58] The iterative process continues until the software's performance meets the desired metrics, at which point the software can be applied to the universe of documents for production.

The computer learns by applying a mathematical algorithm to a data set.[59] Two common types of algorithms are latent semantic indexing and naïve Bayes algorithms.[60] Latent semantic indexing essentially uses decision trees to look for a keyword or phrase that distinguishes responsive and non-responsive documents, based on a pre-coded set.[61] Naïve Bayes algorithms categorize documents based on word use, and in practice tend to work much like a keyword

47. *See, e.g.*, Matthew D. Nelson, Predictive Coding for Dummies 7–8 (2012).
48. *Id.* at 15.
49. *Id.*
50. *Id.* at 16.
51. *Id.*
52. *Id.*
53. *Id.* at 17.
54. *Id.*
55. *Id.* at 18.
56. *Id.*
57. *Id.*
58. *Id.*
59. Tim Leehealey, *The Machine Learning/Predictive Coding Silver Bullet*, eDiscovery Insight (Sept. 24, 2012), http://ediscoveryinsight.com/2012/09/the-machine-learningpredictive-coding-silver-bullet.
60. *Id.*
61. *Id.*

search.[62] In *Da Silva Moore*, the software used both Support Vector Machines, a latent semantic algorithm, and Probabilistic Latent Semantic Analysis, a naïve Bayes algorithm.[63]

III. Proportionality and Developments in the Federal System

A. Proportionality and the Federal Rules: Getting Lawyers to Play Nice with Others

Rule 26(b)(2)(C)(iii) provides that "the court must limit the frequency or extent of discovery . . . if it determines that . . . the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues."[64] That is the proportionality standard.[65]

As discussed above, in *In re Biomet M2a Magnum Hip Implant Products Liability Litigation*, the court invoked Rule 26(b) in determining whether to order defendant Biomet to re-run its production, using predictive coding on the entire universe of documents.[66] The court noted that "it would cost Biomet a million, or millions, of dollars to test [plaintiffs'] theory that predictive coding would produce a significantly greater number of relevant documents."[67] The court concluded that, "[e]ven in light of the needs of the hundreds of plaintiffs in this case, the very large amount in controversy, the parties' resources, the importance of the issues at stake, and the importance of this discovery in resolving the issues," the likely benefits would not equal or outweigh the costs.[68]

Similarly, in *ADT Security Services, Inc. v. Pinnacle Security, LLC*,[69] Chief Judge Holderman invoked the proportionality principle to affirm a ruling on a motion to compel. Plaintiff sought to compel defendant to re-do an ESI search, asserting that documents seemed to be missing based on the disparity in the volume of documents produced by the parties.[70] Magistrate Judge Kim granted limited relief, ordering Pinnacle to re-do its search with respect to seven employees' com-

62. *Id.*

63. James Hanft, *Technology: Shedding Light on the Predictive Coding Black Box,* Inside Couns. (Mar. 16, 2012), http://www.insidecounsel.com/2012/03/16/technology-shedding-light-on-the-predictive-coding.

64. Fed. R. Civ. P. 26(b)(2)(C)(iii).

65. The Standing Committee on Rules of Practice and Procedure of the United States Courts is considering amendments to the federal discovery rules, including Rules 26 and 37. Henry Kelston, *Are We on the Cusp of Major Changes to E-Discovery Rules?*, Law Tech. News (Apr. 17, 2013), http://goo.gl/CYpHf3. The revisions would modify Rule 26(b)(1) to restrict the scope of discovery so that it is "proportional to the needs of the case," based on the factors set out in Rule 26(b)(2)(C). *Id.*; *see also CCL Addresses Federal Civil Rules Advisory Committee*, Ctr. for Const. Litig. (Apr. 17, 2013), http://www.cclfirm.com/blog/8333/ (charting proposed changes to the rules under consideration).

66. *In re* Biomet M2a Magnum Hip Implant Prods. Liab. Litig., No. 3:12-MD-2391, slip op. at 3–4 (N.D. Ind. Apr. 18, 2013) (order regarding discovery of ESI).

67. *Id.* at 6.

68. *Id.*

69. No. 10 C 7467, 2012 U.S. Dist. LEXIS 98948 (N.D. Ill. July 11, 2012).

70. *Id.* at *5.

puters for which there was evidence that they contained correspondence missing from the initial discovery production.[71] Chief Judge Holderman affirmed, noting that plaintiff's broadly worded inquiries "violate[d] the principle that '[t]o further the application of the proportionality standard in discovery, requests for production of ESI and related responses should be reasonably targeted, clear, and as specific as practicable.'"[72]

Conversely, in *Chen-Oster v. Goldman, Sachs & Co.*,[73] the court applied Rule 26(b)(2)(C) to direct extensive further discovery. There, plaintiffs sought database information dating back as far as twelve years.[74] Defendant objected based on phasing, accessibility, and proportionality arguments, contending that it would take hundreds of hours to extract and check the requested data.[75] The court noted that either sampling or a mass production of all data contained in the databases would resolve the issue, although neither party had endorsed those options.[76] Concluding that the information sought was central to the case, the amount in controversy was substantial, that defendant's resources were ample, and the litigation was important, the court granted the motion to compel.[77]

B. A Principled Approach to Proportionality: The Seventh Circuit Electronic Discovery Pilot Program's Proposed Case Management Orders

In an effort to provide concrete guidance in implementing the proportionality principle, the Seventh Circuit Electronic Discovery Pilot Program has proposed two case management orders to address issues related to the collection and production of ESI.

The first proposal, a Discovery Plan for Electronically Stored Information (the "Discovery Plan"), is a "framework that may be used by parties in cases with either limited or extensive discovery" of ESI.[78] The Discovery Plan follows from Rule 26 and Principle 2.01 of the Seventh Circuit Electronic Discovery Pilot Program, and it addresses scope, searching, production format, and third-party ESI.[79] It makes clear that the "parties are aware of the importance the Court places on cooperation and commit to cooperate in good faith" and that nothing

71. *Id.* at *6.

72. *Id.* at *7 (quoting Seventh Cir. Elec. Discovery Pilot Program Comm., Phase One: October 1, 2009–May 1, 2010: Statement of Purpose and Preparation of Principles 11 (Oct. 1, 2009) (setting forth Principle 1.03 of *Principles Relating to the Discovery of Electronically Stored Information* to be implemented and evaluated during the Phase One period from October 1, 2009 through May 1, 2010)).

73. 285 F.R.D. 294 (S.D.N.Y. 2012).

74. *Id.* at 297.

75. *Id.* at 303–04.

76. *Id.* at 304–05.

77. *Id.* at 305–06, 308.

78. Seventh Cir. Elec. Discovery Pilot Program Comm., Interim Report on Phase Three: May 2012–May 2013 app. A, at 54 (2013), *available at* http://www.discoverypilot.com/sites/default/files/phase_three_interim_report.pdf.

79. *Id.* at 55–61.

in the Discovery Plan "shall supersede the provisions of any subsequent Stipulated Protective Order."[80] The Discovery Plan limits the scope of document collection to an agreed time range and allows for additional limitations, for example based on geographic or organizational factors.[81] The Discovery Plan also distinguishes between cases with limited and extensive ESI.[82] For cases with extensive ESI, the Discovery Plan: (1) addresses the types of e-mail and unstructured data (like word documents or spreadsheets), custodians, and shared data to be produced, and provides for a search protocol that sets out whether technology-assisted review, like predictive coding, will be used;[83] (2) deals with the format for production materials, including metadata, load files, and de-duplication, as well as whether documents without standard pagination, like spreadsheets, will be produced in native, single page TIFs, or hard copy;[84] and (3) calls on each party to identify a knowledgeable e-discovery liaison.[85]

The second proposed order addresses privilege and work-product issues.[86] The proposed order requires a party that withholds ESI based on privilege to provide a spreadsheet listing the ESI withheld, with as much metadata as is reasonably available and a description of the categories of ESI being withheld.[87] The proposed order then provides a process for challenging privilege designations.[88] Finally, the proposed order includes a non-waiver and clawback protocol, specifying that production, whether inadvertent or intentional, does not waive any privilege.[89] The proposed order allows a producing party to assert the privilege "at any time," although affirmative use of a produced document waives any privilege as to that document.[90]

IV. Conclusion

With electronic discovery now a fact of everyday life, courts are moving to address the resulting cost and burden by more aggressively using the proportionality principle, even as technological advances like predictive coding increase the range of cost-saving measures available to attorneys. Both of those developments seem likely to continue in the future.

80. *Id.* at 55.
81. *Id.* at 55–56.
82. *Id.* at 56.
83. *Id.* at 56–57.
84. *Id.* at 58–60.
85. *Id.* at 61.
86. *Id.* app. B, at 68.
87. *Id.*
88. *Id.* at 69.
89. *Id.*
90. *Id.*

Virtual Uncertainty: Developments in the Law of Electronic Payments and Financial Services

By Stephen T. Middlebrook and Sarah Jane Hughes***

I. Introduction

The past year has seen significant legal changes concerning electronic payments and financial services. Some have resolved ambiguity, while others have increased uncertainty for those operating in these areas. Part II of this survey covers developments relating to virtual currencies, undoubtedly the most controversial and significant area this year. Part III looks at the efforts of the Consumer Financial Protection Bureau ("CFPB") to tweak the cross-border remittance transfer rule that the 2012 survey discussed.[1] Part IV reviews the CFPB's first use of its preemption authority in determinations that void parts of Tennessee's gift card escheat law,[2] while leaving a similar Maine law[3] in force.[4] Part V briefly covers the first enforcement action by the Federal Deposit Insurance Corporation ("FDIC") against a bank for unsafe and unsound banking practices, unfair or deceptive practices, and more in connection with its prepaid card business.[5] Part VI sets forth some conclusions about the manner in which the federal government appears to be approaching the regulation of e-payments and financial services.

* Stephen T. Middlebrook is the General Counsel of FSV Payment Systems, Inc., a prepaid processor and program manager. Prior to joining FSV, he was Senior Counsel at the U.S. Department of the Treasury, Financial Management Service. He is the current co-chair of the Electronic Payments and Financial Services Subcommittee of the Cyberspace Law Committee. He can be reached at stm@aol.com. The views contained in this survey are his and may not reflect the views of his employer.

** Sarah Jane Hughes is the University Scholar and Fellow in Commercial Law at the Maurer School of Law at Indiana University. She is a former co-chair of the Electronic Payments and Financial Services Subcommittee of the Cyberspace Law Committee and that Committee's current publications chair. She can be reached at sjhughes@indiana.edu. The views contained in this survey do not reflect the views of the Maurer School of Law or the Trustees of Indiana University.

1. 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).

2. Tenn. Code Ann. § 66-29-135(a) (2004).

3. Me. Rev. Stat. Ann. tit. 33, §§ 1961(2), 1962 (2012).

4. Electronic Fund Transfers; Determination of Effect on State Laws (Maine and Tennessee), 78 Fed. Reg. 24386, 24390 (Apr. 25, 2013).

5. *See infra* notes 79–87 and accompanying text.

II. Recent Developments in the Regulation of Virtual Currencies

The legal landscape for virtual currencies remained undisturbed from when we last wrote about the subject in 2008[6] until early 2013, when both regulators and law enforcement turned their attention to these alternative payment systems. Their actions were likely influenced by growing usage of virtual currencies, especially Bitcoin.[7] The Financial Crimes Enforcement Network ("FinCEN") issued guidance clarifying the application of anti-money laundering rules to virtual currencies ("FinCEN Guidance").[8] That guidance was followed by two significant law enforcement actions. First, the Department of Homeland Security ("DHS") seized funds belonging to Mt. Gox, a major Bitcoin exchange.[9] Shortly thereafter, the Department of Justice ("DOJ") indicted Liberty Reserve, a major international digital currency company, and its principals, on charges of money laundering.[10] Subpart A of this section evaluates the FinCEN Guidance. Subpart B covers DHS's seizure of Mt. Gox's funds; and Subpart C covers the DOJ's indictment of Liberty Reserve.

A. FinCEN Issues New Guidance on Virtual Currencies

On March 18, 2013, FinCEN issued interpretive guidance clarifying the application of the Bank Secrecy Act to virtual currencies.[11] FinCEN had previously promulgated regulations governing money services businesses ("MSBs"), including currency exchanges and money transmitters, which are obligated to comply with registration, record-keeping, and other requirements ("MSB Rule").[12] This new guidance attempts to clarify if and when participants in virtual currency transactions might be engaging in "money transmission" and thus subject to the MSB Rule.

6. Patricia Allouise, Sarah Jane Hughes & Stephen T. Middlebrook, *Developments in the Laws Affecting Electronic Payments and Stored-Value Products: A Year of Stored-Value Bankruptcies, Significant Legislative Proposals, and Federal Enforcement Actions*, 64 Bus. Law. 219 (2008) [hereinafter *2008 Survey*].

7. Bitcoin is a virtual currency that is supported by a peer-to-peer network and has no central issuing authority. *See generally* Eur. Cent. Bank, Virtual Currency Schemes 21–26 (Oct. 2012), *available at* http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

8. Fin. Crimes Enforcement Network, U.S. Dep't of the Treasury, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013) [hereinafter FinCEN Guidance], *available at* http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.

9. Joe Mullin, *Feds Seize Money from Dwolla Account Belonging to Top Bitcoin Exchange Mt. Gox,* Ars Technica (May 14, 2013, 5:55 PM), http://arstechnica.com/tech-policy/2013/05/feds-seize-money-from-top-bitcoin-exchange-mt-gox/.

10. Press Release, U.S. Attorney's Office, Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One of World's Largest Digital Currency Companies, and Seven of Its Principals and Employees for Allegedly Running a $6 Billion Money Laundering Scheme (May 28, 2013), *available at* http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php.

11. FinCEN Guidance, *supra* note 8, at 1.

12. Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses, 76 Fed. Reg. 43585 (July 21, 2011) (to be codified at 31 C.F.R. pts. 1010, 1021 & 1022).

FinCEN begins its guidance by distinguishing "real" currency from "virtual" currency. Real currency is the coin and paper money of the United States, or another country, that has the status of legal tender in the country of issue.[13] Virtual currency does not have legal tender status and thus is not real currency. Some virtual currency, however, has an equivalent value in real currency or may be used as a "substitute" for real currency, and FinCEN deems this "convertible virtual currency."[14] FinCEN is not explicit on this point, but presumably a virtual currency such as Bitcoin that can be exchanged for real currency would constitute a convertible virtual currency.

Because convertible forms of virtual currency may "substitute" for real currency, a transaction in these virtual currencies may qualify as a "money transmission." FinCEN defines "money transmission" as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[15] Whether a particular entity is or is not a "money transmitter" is "a matter of facts and circumstances," but the rules set forth a number of specific exemptions.[16] A person who takes a convertible virtual currency from one person and then transmits that convertible virtual currency to another person or location would be a "money transmitter," according to the FinCEN Guidance.[17]

The FinCEN Guidance next divides participants in virtual currency arrangements into three categories: users, exchangers, and administrators.[18] "Users" obtain virtual currency in order to purchase real or virtual goods and services.[19] "Exchangers" engage in the exchange of virtual currency for real or virtual currency as a business.[20] "Administrators" engage in the business of issuing and redeeming virtual currency.[21] Users are not MSBs because they do not transmit the value of funds to another person or location.[22] An exchanger or administrator will be a "money transmitter" if it (1) accepts and transmits a convertible virtual currency between persons or from one location to another,[23] or (2) buys or sells convertible virtual currency, unless, in either case, an exemption applies.[24] An intermediary that accepts and transmits funds solely for the purpose of completing a bona fide purchase or sale of currency—real or virtual—is exempt and will not be treated as a "money transmitter."[25] However, FinCEN views an

13. FinCEN Guidance, *supra* note 8, at 1.
14. *Id.*
15. 31 C.F.R. § 1010.100(ff)(5)(i)(A) (2013) (defining "money transmission services").
16. *Id.* § 1010.100(ff)(5)(i)(B)(ii).
17. FinCEN Guidance, *supra* note 8, at 3.
18. *Id.* at 2.
19. *Id.*
20. *Id.*
21. *Id.*
22. *Id.*
23. *Id.* at 4.
24. *Id.* at 3.
25. *Id.*

exchange that takes funds from a user and then transmits those funds to the user's account at the administrator to be engaged in "money transmission."[26]

In a virtual currency system such as Bitcoin, which operates without a central administrator, a person who creates units of the virtual currency (a "miner" in Bitcoin parlance) and uses it to purchase real or virtual goods is merely a user and would not be a "money transmitter."[27] In contrast, FinCEN clarifies that "a person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter."[28] Thus, a Bitcoin "miner" who creates and sells Bitcoins for real currency is apparently a "money transmitter." However, FinCEN's definitions of both an "exchanger" and an "administrator" contain the phrase "engaged as a business,"[29] which is not defined. It is unclear at what point an entity participating in the virtual currency market would be deemed to be "engaged as a business," and thus it is difficult to advise when the MSB Rule begins to apply.

While the FinCEN Guidance does not specifically reference Bitcoin, the applicable rules have drawn criticism from Bitcoin proponents. For example, Patrick Murck, legal counsel for the Bitcoin Foundation that promotes use of the virtual currency, said that the FinCEN Guidance "would be infeasible for many, if not most, members of the Bitcoin community to comply with."[30] At least three "exchanges" that traded Bitcoins shut down shortly after the new guidance was issued.[31] Treasury Undersecretary David Cohen stated that virtual currency exchanges that comply with the law "have nothing to fear from Treasury."[32] Given compliance challenges, however, those exchanges are unlikely to find much comfort in Cohen's statement.

B. Homeland Security Seizes Funds Held by Bitcoin Exchange Mt. Gox

On May 14, 2013, DHS obtained a seizure warrant directed to Dwolla, an Iowa-based internet payments company, ordering the seizure and forfeiture of an account belonging to Mutum Sigillum, LLC.[33] According to the affidavit of

26. *See id*. at 4.

27. *See id*. at 5. How one obtains virtual currency may be described using various terms—such as "mining"—depending on the specific virtual currency model. *See id*. at 2 n.7.

28. *Id*. at 5.

29. *Id*. at 2.

30. Jeffrey Sparshott, *Web Money Gets Laundering Rule*, Wall St. J. (Mar. 21, 2013), http://online.wsj.com/article/SB10001424127887324373204578374611351125202.html.

31. Jon Matonis, *FinCEN's New Regulations Are Choking Bitcoin Entrepeneurs*, Am. Banker (Apr. 25, 2013, 10:00 AM), http://www.americanbanker.com/bankthink/fincen-regulations-choking-Bitcoin-entrepreneurs-1058606-1.html.

32. *Liberty Reserve Case No Comment on e-Currency Exchangers*, United Press Int'l (May 29, 2013, 3:30 AM), http://www.upi.com/Business_News/2013/05/29/US-Liberty-Reserve-case-no-comment-on-e-currency-exchangers/UPI-50571369812600/.

33. Seizure Warrant at 1, *In re* Contents of One Dwolla Account, No. 13-1162 SKG (D. Md. May 14, 2013), *available at* http://cdn.arstechnica.net/wp-content/uploads/2013/05/Mt-Gox-Dwolla-Warrant-5-14-13.pdf; *see also* Mullin, *supra* note 9.

a federal agent filed with the warrant application, Mutum Sigillum is the U.S.-based subsidiary of Mt. Gox, which is the world's largest Bitcoin exchange and which is based in Japan.[34] The affidavit stated that a confidential informant residing in Maryland established an account at Dwolla that he used to fund an account at Mt. Gox and to purchase Bitcoins.[35] In addition, the informant also exchanged Bitcoins for U.S. dollars that were transmitted back to him through Mutum Sigillum and Dwolla accounts.[36] Apparently relying upon, but not citing to, the FinCEN Guidance, DHS asserted that those transactions demonstrated that Mutum Sigillum was engaged in "money transmission."[37] The affidavit noted that Mutum Sigillum was not registered with FinCEN as required by 31 U.S.C. § 5330, and asserted that Mt. Gox consequently was in violation of 18 U.S.C. § 1960 and subject to legal penalties.[38] One such penalty is the forfeiture of property as authorized by 18 U.S.C. § 981(a)(1)(A).[39] The affidavit noted that Mutum Sigillum funds were also transmitted through an account at Wells Fargo and that a separate warrant was issued to seize funds in that account.[40] While law enforcement executed warrants to seize the funds of Mt. Gox located in the United States, as of June 12, 2013, no indictments of Mt. Gox or its subsidiary Mutum Sigillum have been handed down. Mt. Gox subsequently implemented a new policy requiring identity verification before it would perform currency deposits or withdrawals.[41]

C. Department of Justice Indicts Liberty Reserve for Money Laundering

On May 28, 2013, the U.S. Attorney for the Southern District of New York unsealed a criminal indictment charging Liberty Reserve and seven of its principals and employees with operating as an unlicensed money transmitter and engaging in money laundering.[42] The indictment charges the defendants under 18 U.S.C. § 1960 with operating an unlicensed money transmitting business in violation of 31 U.S.C. § 5330 and its accompanying regulations.[43] Defendants

34. Affidavit in Support of Seizure Warrant at 2, *In re* Contents of One Dwolla Account, No. 13-1162 SKG (D. Md. May 14, 2013), *available at* http://cdn.arstechnica.net/wp-content/uploads/2013/05/Mt-Gox-Dwolla-Warrant-5-14-13.pdf.

35. *Id.* at 3.

36. *Id.*

37. *Id.*

38. *Id.* at 1–2.

39. *Id.* at 4–5.

40. *Id.* at 4; *see also* Brian Browdie, *Bitcoin Exchange in U.S. Crosshairs Banked at Wells Fargo*, Am. Banker (May 16, 2013, 8:43 AM), http://www.americanbanker.com/issues/178_95/Bitcoin-exchange-in-u-s-crosshairs-banked-at-wells-fargo-1059158-1.html.

41. Press Release, Mt. Gox, Statement Regarding Account Verifications (May 30, 2013), *available at* https://mtgox.com/press_release_20130530.html. For more information, see Andy Greenberg, *Not So Anonymous: Bitcoin Exchange Mt. Gox Tightens Identity Requirement*, Forbes (May 30, 2013, 12:03 PM), http://www.forbes.com/sites/andygreenberg/2013/05/30/not-so-anonymous-bitcoin-exchange-mt-gox-tightens-identity-requirement/.

42. Press Release, U.S. Attorney's Office, *supra* note 10.

43. Indictment ¶¶ 41–42, United States v. Liberty Reserve, S.A., 13 Crim. 368 (S.D.N.Y. 2013), *available at* http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR/Liberty%20Reserve,

were also charged with conspiracy to commit money laundering in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 1956(a)(2)(B)(i).[44] Liberty Reserve is alleged to have been a "financial hub of the cyber-crime world, facilitating . . . credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking."[45] The government estimated that Liberty Reserve had 200,000 users in the United States and processed over twelve million transactions a year with a value of more than $1.4 billion.[46]

Allegedly, Liberty Reserve did not require users to validate their identity, and criminals created accounts under false names such as "Russian Hackers."[47] The government alleges that Liberty Reserve, in an effort to add an additional layer of anonymity, did not permit users to transmit funds directly to Liberty Reserve, but instead required them to make deposits and withdrawals through third-party exchanges.[48] Liberty Reserve allegedly recommended third-party exchanges that tended to be unlicensed money transmitters operating without government oversight and that were concentrated in Malaysia, Russia, Nigeria, and Vietnam.[49] Pursuant to 18 U.S.C. § 982(a)(1), the government seeks forfeiture of "at least $6 billion" held in accounts in Costa Rica, Cyprus, Russia, Hong Kong, China, Morocco, Spain, Latvia, and Australia, as well as one account at SunTrust Bank in the United States.[50]

Of special interest to followers of cyberspace law, in a declaration filed in support of a post-indictment restraining order, seizure warrant, and injunction against Liberty Reserve, a Secret Service agent stated that the investigation included execution of "one of the first-ever 'cloud'-based search warrants, directed to a service provider used to process Liberty Reserve's Internet traffic."[51] The government also sought an injunction preventing Amazon Web Services from providing services to support Liberty Reserve's website.[52]

On the same day that indictment was unsealed, FinCEN issued a notice of proposed rulemaking to declare Liberty Reserve an institution of primary money laundering concern under section 311 of the Patriot Act.[53] The rule would prohibit all U.S. financial institutions from maintaining correspondent relationships with foreign banks that do business with Liberty Reserve.[54]

%20et%20al.%20Indictment%20-%20Redacted.pdf. The charges also include conspiracy to operate an unlicensed money transmitter business. *Id.* ¶¶ 33–40.

44. *Id.* ¶¶ 1–32.
45. *Id.* ¶ 9.
46. *Id.* ¶ 10.
47. *Id.* ¶¶ 14 & 19.
48. *Id.* ¶ 16.
49. *Id.* ¶ 18.
50. *Id.* ¶ 43.
51. Declaration of Special Agent [redacted] in Support of Ex Parte Application for Post-Indictment Restraining Order, Seizure Warrant, and Injunction Pursuant to 21 U.S.C. § 853(e) and (f) ¶ 9, United States v. Liberty Reserve, S.A., 13 Crim. 368 (S.D.N.Y. 2013), *available at* http://goo.gl/ba29WV.
52. *Id.* ¶ 74.
53. Imposition of Special Measure Against Liberty Reserve S.A. as a Financial Institution of Primary Money Laundering Concern, 78 Fed. Reg. 34008 (proposed June 6, 2013) (to be codified at 31 C.F.R. pt. 1010).
54. *See id.* at 34009.

The measure would effectively cut off Liberty Reserve from the U.S. financial system.[55]

While the Mt. Gox forfeiture order and the Liberty Reserve criminal indictment are quite different on a number of levels, both use 18 U.S.C. § 1960 to enforce the registration requirement for MSBs with severe penalties, including asset forfeiture and additional criminal sanctions. Prosecutors employed essentially the same strategy against e-Gold, which we described and critiqued in prior surveys.[56] These actions, following so soon after the publication of the FinCEN Guidance, signal the government's intent to police the virtual currency market robustly. These methods may be a convenient and effective way for law enforcement to deal with money launderers, but they have potentially significant collateral effects on small companies and start-ups that wish to operate within the confines of the law, but lack the resources or the expertise to navigate such tricky regulatory waters. Establishing appropriate compliance obligations without stifling innovation in emerging payments technology is always a concern. With regard to virtual currencies, it remains to be seen whether the government has found the proper balance.

III. The CFPB Tweaks and Re-Tweaks the "Remittance Transfer" Rule

Responding to industry concerns,[57] the CFPB has tweaked its February 2012 rule amending Regulation E ("2012 Remittance Rule")[58] to implement the cross-border remittance transfer provisions of Dodd-Frank Act's section 1073[59] on several occasions.[60] On May 22, 2013, the CFPB amended the 2012 Remittance

55. Chris Cumming, *FinCEN Seeks to Deputize Banks in $6B Laundering Case*, Am. Banker (May 28, 2013, 5:59 PM), http://www.americanbanker.com/issues/178_102/fincen-seeks-to-deputize-banks-in-6-billion-laundering-case-1059434-1.html.

56. *2008 Survey, supra* note 6, at 248–50; Sarah Jane Hughes, Stephen T. Middlebrook & Broox W. Peterson, *Developments in the Law Concerning Stored-Value Cards and Other Electronic Payments Products*, 63 Bus. Law. 237, 255–62 (2007).

57. *See, e.g.*, Becky Nelson, *CFPB Updates Remittance Rules,* CFPB J. (Feb. 8, 2012), http://cfpbjournal.com/issue/cfpb-journal/article/cfpb-updates-remittance-rules; *CU Remittance Concerns Aired at D.C. Symposium,* Credit Union Nat'l Ass'n (Apr. 20, 2012), http://www.cuna.org/Stay-Informed/News-Now/Washington/CU-remittance-concerns-aired-at-D-C–symposium/?CollectionId=5; 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), *available at* http://www.theclearinghouse.org/index.html?f=073844.

58. Electronic Fund Transfers (Regulation E), 77 Fed. Reg. 6194 (Feb. 7, 2012) (to be codified at 12 C.F.R. pt. 1005). The 2012 Cyberspace Law Survey analyzed the 2012 Remittance Rule. Hughes, *supra* note 1, at 234–37.

59. Dodd-Frank Wall Street Reform and Consumer Protection Act § 1073, 15 U.S.C. § 1693o-1 (2012).

60. Electronic Fund Transfers (Regulation E), 78 Fed. Reg. 30662 (May 22, 2013) (to be codified at 12 C.F.R. pt. 1005) (promulgating amendments and announcing effective date of October 28, 2013); Electronic Fund Transfers (Regulation E) Temporary Delay of Effective Date, 78 Fed. Reg. 6025 (Jan. 29, 2013) (postponing effective date from February 7, 2013 until amendments proposed in December 2012 are promulgated); Electronic Fund Transfers (Regulation E), 77 Fed. Reg. 77188 (proposed Dec. 31, 2012) (to be codified at 12 C.F.R. pt. 1005) (proposing additional flexibility regarding the disclosure of foreign taxes and revisions to the error resolution procedures); Electronic

Rule in three major respects.[61] These May 2013 amendments (1) permit disclosure of fees imposed and taxes to be collected by any person other than the remittance transfer provider; (2) require disclaimers indicating that the recipient may receive less than the disclosed total, due to the fees and taxes for which disclosure is now optional; and (3) exempt transactions from the error provision requirements if funds are deposited into an account other than that of the intended recipient because the consumer-sender supplied an incorrect account number or recipient institution identifier.[62]

IV. The CFPB Preempts Gift Card Escheat Laws in Tennessee but Not Maine

The Credit Card Accountability Responsibility and Disclosure Act of 2009 ("Credit CARD Act")[63] amended the Electronic Fund Transfer Act ("EFTA"),[64] among other things, to prohibit expiry of funds underlying gift cards before the later of five years from the date of initial issuance of the card or the date of the last funds loaded onto the card.[65] The EFTA preempts state laws only to the extent of inconsistency with its provisions, unless the state law is more protective of consumers.[66]

Many states require escheat of unused and dormant balances on gift cards as quickly as two years after issuance or the last value is added to the card.[67]

Fund Transfers (Regulation E), 77 Fed. Reg. 50244 (Aug. 20, 2012) (to be codified at 12 C.F.R. pt. 1005) (exempting providers of 100 or fewer remittance transfers in each of the previous calendar year and the current calendar year and offering a six-month transition period for providers that cross the 100-transaction threshold to come into full compliance with subpart B of Regulation E); Electronic Fund Transfers (Regulation E), 77 Fed. Reg. 6310 (proposed Feb. 7, 2012) (to be codified at 12 C.F.R. pt. 1005) (proposing exclusion from definition of "remittance transfer provider" of companies that do not provide remittance transfers "in the normal course of business" and refining requirements for "preauthorized" remittance transfers that are scheduled to recur at substantially regular intervals).

61. Electronic Fund Transfers (Regulation E), 78 Fed. Reg. at 30662.

62. *Id.* The exemption is subject to notice to the consumer-sender prior to the transfer that the funds could be lost and to reasonable procedures and efforts to verify the accuracy of the recipient institution's identifying information and to retrieve funds misdirected as a result of incorrect information from senders. *Id.*

63. Pub. L. No. 111-24, 123 Stat. 1734 (2009) (codified in scattered sections of 15 U.S.C.).

64. 15 U.S.C. §§ 1693–1693r (2012).

65. Credit CARD Act, *supra* note 63, § 401, 123 Stat. at 1753 (codified at 15 U.S.C. 1693*l*-1(c)(2)(A) (2012)); *see also* 12 C.F.R. § 1005.20(e)(2)(i) (2013). The original effective date of the prohibition was fifteen months after enactment. Credit CARD Act § 403, *supra* note 63, 123 Stat. at 1754 (codified at 15 U.S.C. § 1693*l*-1 note (2012)).

66. 15 U.S.C. § 1693q (2012).

67. *See* Electronic Fund Transfers; Determination of Effect on State Laws (Maine and Tennessee), 78 Fed. Reg. 24386, 24387 (Apr. 25, 2013). The CFPB also observed that, following transfer of abandoned funds to a state, "[i]f the gift card holder . . . seeks to use the card, State law typically permits—but does not necessarily require—the gift card issuer to honor the card and to seek reimbursement from the State. If the gift card issuer opts not to honor the card, the gift card owner can contact the State to attempt to reclaim the property." *Id.* at 24387–88. For more analysis of state escheat laws and related gift card litigation, see Hughes, *supra* note 1, at 241–42; Sarah Jane Hughes, *Developments in the Laws Governing Electronic Payments*, 67 Bus. Law. 259, 277–78 (2011); Sarah Jane Hughes & Stephen T. Middlebrook, *Developments in the Laws Governing Electronic Payments Made Through Gift*

These escheat laws conflict with the Credit CARD Act if, after remitting unused balances to the state, issuers refuse to honor cards. In April 2013, the CFPB determined that the EFTA preempted section 66-29-116 of Tennessee's Uniform Disposition of Unclaimed Property Act[68] because that section allowed issuers to decline to honor cards as soon as two years after issuance and relieved them of liability to consumers.[69] The CFPB concluded that Tennessee's law "permit[s] cards and their underlying funds to expire sooner than is permitted under the EFTA and Regulation E."[70]

Maine similarly relieves gift card issuers from liability to card owners after issuers transfer underlying funds to the State.[71] The CFPB, however, did not preempt Maine's statute,[72] relying on "communications" with the Office of the State Treasurer ("Maine's Treasurer") that it instructs gift card issuers who transfer unclaimed funds to the State to honor cards on subsequent presentation "indefinitely" and then to request reimbursement from the State.[73] Maine's Treasurer apparently persuaded the CFPB that its consumers could use their gift cards for at least as long as they are guaranteed that right by the EFTA and Regulation E.[74] Commentators described the CFPB's rationale for not preempting Maine's law as "novel"[75] or used words of similar import.[76]

Those commentators criticized the CFPB's position that issuers who honor cards should look to the state for reimbursement of abandoned funds previously transferred to the state.[77] Some commentators observed that card issuers will be

Cards, Debit and Prepaid Cards, and Direct Deposits of Federal Benefits, 66 BUS. LAW. 159, 160–67 (2010).

68. TENN. CODE ANN. § 66-29-135(a) (2004) (providing that card is presumed abandoned if unclaimed two years from issuance); *id.* § 66-29-116 ("Any person who pays or delivers abandoned property to the treasury . . . is relieved of all liability . . . which thereafter may arise . . . in respect of the property."). For discussion of the CFPB's view of Tennessee's law pertaining to cards that cannot be used at multiple, unaffiliated merchants or at automated teller machines, see Electronic Fund Transfers; Determination of Effect on State Laws (Maine and Tennessee), 78 Fed. Reg. at 24390.

69. Electronic Fund Transfers; Determination of Effect on State Laws (Maine and Tennessee), 78 Fed. Reg. at 24390–91.

70. *Id.* at 24391; *see also* 12 C.F.R. § 1005.20(e)(2)(i) (2013) (prohibiting expiry in less than five years).

71. *See* ME. REV. STAT. ANN. tit. 33, § 1961(2) (2012) ("A holder who pays or delivers property to the administrator in good faith is relived of all liability arising thereafter with respect to the property.").

72. Electronic Fund Transfers; Determination of Effect on State Laws (Maine and Tennessee), 78 Fed. Reg. at 24387.

73. *Id.* at 24389–90.

74. *Id.* at 24390.

75. Rick Fischer, Obrea Poindexter, Leonard Chanin & Matt Janiga, *CFPB Uses Novel Interpretation, Increases Compliance Burden for Gift Card Issuers Through Its First Preemption Decision*, MORRISON FOERSTER, 1 (Apr. 23, 2013), http://www.mofo.com/files/Uploads/Images/130423-CFPB-Gift-Card-Issuers.pdf.

76. Margo Hirsch Strahlberg & Judith Rinearson, *CFPB Issues Preemption Determination Regarding State Unclaimed Property Laws*, BRYAN CAVE FIN. SERVICES GROUP, 2 (Apr. 24, 2013), http://goo.gl/V2oXg6 (noting that all twenty public comments delivered to the CFPB supported preemption).

77. *See* Fischer, Poindexter, Chanin & Janiga, *supra* note 75, at 3; Strahlberg & Rinearson, *supra* note 76, at 2.

required to pay "twice the value of funds . . . loaded"—once to the state and again to the card holder—and then seek reimbursement from the state.[78]

V. The FDIC's Enforcement of Treasury's "Federal Benefits" Rule Extends Regulation E's Payroll Card Provisions to General Purpose Prepaid Cards that Contain Federal Benefits

On May 31, 2013, the FDIC announced settlements with a bank and an affiliated prepaid card issuer for violations of the Treasury Rule, 31 C.F.R. § 210, which governs the use of the Automated Clearing House system to deliver federal benefit payments to prepaid debit cards.[79] The FDIC determined that First California Bank ("FCB") and its institution-affiliate, Achieve Financial Services, LLC ("Achieve"), engaged in unfair and deceptive practices in the marketing and servicing of a prepaid, reloadable credit card.[80] The consent orders require FCB and Achieve to comply with the Treasury Rule (including protections afforded by Regulation E),[81] the guidance offered by the FDIC and the Federal Reserve regarding unfair or deceptive practices,[82] and section 5 of the Federal Trade Commission Act,[83] and also to implement extensive auditing and compliance programs.[84] FCB agreed to pay a civil penalty of $600,000 to the FDIC[85] and to oversee (and effectively guarantee) restitution of $1,110,000 for consumers who used prepaid products marketed by two card issuers.[86] The consent orders effectively establish Regulation E's rules for "payroll cards" as the standard for general-purpose reloadable ("GPR") cards.[87] As a result, it may reduce the

78. Fischer, Poindexter, Chanin & Janiga, *supra* note 75, at 3.

79. Press Release, Fed. Deposit Ins. Corp., FDIC Announces Settlements with First California Bank (FCB), Westlake Village, California, and Achieve Financial Services, LLP (Achieve), Austin, Texas (May 31, 2013), *available at* http://fdic.gov/news/news/press/2013/pr13045.html.

80. *Id.*

81. 12 C.F.R. pt. 1005 (2013).

82. Bd. of Governors of the Fed. Reserve Sys. & Fed. Deposit Ins. Corp., Unfair or Deceptive Acts or Practices by State-Chartered Banks, FIL-26-2004 (Mar. 11, 2004), *available at* http://fdic.gov/news/news/financial/2004/fil2604a.html.

83. 15 U.S.C. § 45 (2012).

84. Consent Order, Order for Restitution, and Order to Pay Civil Money Penalty ¶¶ 2–7, *In re* First Cal. Bank, FDIC-13-046b (May 28, 2013) [hereinafter FCB Consent Order]; Consent Order, Order for Restitution, and Order to Pay Civil Money Penalty ¶¶ 4–13, *In re* Achieve Fin. Servs., LLC, FDIC-13-048b (May 28, 2013).

85. FCB Consent Order, *supra* note 84, ¶ 11.

86. *See id.* ¶ 8 (requiring FCB to establish, and ensure contribution of $1,100,000 to, an Achieve Restitution Account); *id.* ¶ 9 (requiring FCB to establish, and ensure contribution of $10,000 to, a Cornerstone Restitution Account); *id.* ¶ 10 (imposing ultimate responsibility for funding and distributing on FCB).

87. 12 C.F.R. § 1005.2(b)(2) (2013) (defining "payroll card account"). For additional discussion of the application of Regulation E to payroll cards, see Electronic Fund Transfers, 71 Fed. Reg. 51437 (Aug. 30, 2006) (to be codified at 12 C.F.R. pt. 205) (extending Regulation E's coverage to payroll card accounts established through employers and to which recurring transfers of wages are made); Electronic Fund Transfers, 59 Fed. Reg. 10678 (Mar. 7, 1994) (to codified at 12 C.F.R. pt. 205) (extending Regulation E's coverage to electronic benefit transfers issued by government agencies). For additional information on the trend in regulation of benefits paid via prepaid cards and GPR prepaid cards, see Electronic Fund Transfers (Regulation E), 77 Fed. Reg. 30923 (May 24, 2012) (to be

need for CFPB regulations related to GPR cards. It also is the first occasion of which we are aware that an issuer of prepaid cards—FCB—has been pursued for the faults of its third-party program manager.

VI. Conclusion

Despite attempts at clarification, many ambiguities remain following the FinCEN Guidance on virtual currencies and the application of the MSB Rule, as discussed in Part II. In addition to the FinCEN Guidance, virtual currency providers are also facing potential regulation from the Commodity Futures Trading Commission[88] and from the states.[89] These new regulations will add to compliance burdens and present new challenges to these emerging businesses. Prepaid card businesses also will continue to face uncertainty as they try to unravel the limits of the preemption authority of the CFPB under the Credit CARD Act, as discussed in Part IV.[90]

Greater certainty will flow from other 2013 actions by the federal government, including publication of the final rule titled Garnishment of Accounts Containing Federal Benefit Payments,[91] the May 2013 amendments to CFPB's remittance transfer rule described in Part III,[92] and from application of the Treasury Rule and Regulation E's "payroll card" provisions to federal benefits paid via prepaid cards discussed in Part V.[93]

codified at 12 C.F.R. pt. 1005) (providing advance notice of proposed rulemaking concerning GPR prepaid cards); Electronic Fund Transfers, 75 Fed. Reg. 16580 (Apr. 1, 2010) (to be codified at 12 C.F.R. pt. 205) (defining the term "general-use prepaid cards" for Regulation E purposes).

88. Tracy Alloway, Gregory Meyer & Stephen Foley, *US Regulators Eye Bitcoin Supervision*, Fin. Times (May 6, 2013, 7:30 PM), http://goo.gl/R7iBlU.

89. Robin Sidel & Andrew R. Johnson, *'Virtual' Currencies Draw State Scrutiny*, Wall St. J. (May 31, 2013, 8:29 PM), http://online.wsj.com/article/SB10001424127887324682204578517604191541808.html.

90. *See supra* notes 63–78 and accompanying text.

91. 78 Fed. Reg. 32099 (May 29, 2013) (to be codified at 5 C.F.R. pts. 831 & 841, 20 C.F.R. pts. 350, 404 & 416, 31 C.F.R. pt. 212 & 38 C.F.R. pt. 1).

92. *See supra* notes 57–62 and accompanying text.

93. *See supra* notes 79–87 and accompanying text.

Copyrights in Cyberspace—Resales, Reposts, Rebukes

*By Jonathan T. Rubens**

Last year's survey considered copyrightability issues and the mobile device markets (the dispute between Oracle and Google over Java copyright protection); the first sale doctrine and the extent to which it may allow modifying bundled technology or redistribution of products acquired online (*Apple Inc. v. Psystar Corp.* and the Second Circuit's opinion in *John Wiley & Sons, Inc. v. Kirtsaeng*); issues in copyright assignment (*Hermosilla v. Coca-Cola Co.*); and considerations of the illegality of content downloading and efforts to stop it over the BitTorrent network (*Call of the Wild Movie LLC v. Does 1–1,062* and other cases).[1] This year's survey starts with the Supreme Court's reversal of the Second Circuit in *Kirtsaeng*, and then it considers caselaw developments addressing the reposting of online content and judicial responses to overzealous tactics used by some copyright litigants.

How Far Has the Supreme Court Expanded the First Sale Doctrine in *John Wiley & Sons, Inc. v. Kirtsaeng*?

In *John Wiley & Sons, Inc. v. Kirtsaeng*,[2] the Supreme Court reversed the Second Circuit, holding that the first sale doctrine applies to copies of a copyrighted work lawfully made abroad, as well as in the United States.[3] Justice Breyer's majority opinion in *Kirtsaeng* focuses on whether the first sale doctrine, which is an exception to a copyright owner's exclusive right of distribution of a copyrighted work, has a geographic limitation. The first sale doctrine, found in section 109(a) of the Copyright Act, provides that:

> Notwithstanding the provisions of section 106(3) [granting exclusive distribution rights], the owner of a particular copy or phonorecord 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 or phonorecord.[4]

* Jonathan Rubens is the chair of the Cyberspace Law Committee and is co-founder of Javid | Rubens LLP in San Francisco, where his practice includes commercial transactions, emerging companies, business acquisitions, and intellectual property.

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

2. 133 S. Ct. 1351 (2013), *rev'g* 654 F.3d 210 (2d Cir. 2011).

3. *Id.* at 1356.

4. 17 U.S.C. § 109(a) (2012).

The Court ruled that the Second Circuit incorrectly interpreted "lawfully made under this title" in section 109(a) to imply a geographical limitation, i.e., that the first sale doctrine only applies when the works in question were made within the United States.[5] The textbooks at issue were printed in Asia specifically for sale in Europe, Asia, Africa, and the Middle East and with copyright notices purporting to prohibit sale elsewhere.[6] However, the Court found that a nongeographic interpretation of the statute was linguistically consistent with the statute and avoided difficulties involving where the Copyright Act may apply.[7]

The dissent by Justice Ginsburg sticks soundly to what was argued by the U.S. government and may have been the more widely anticipated outcome, i.e., that the circuit court got it right when it followed dictum in *Quality King Distributors v. L'anza Research International Inc.*,[8] which held that a copyright owner's right to control imports under section 602(a)(1) of the Copyright Act is a component of the distribution right set forth in section 106(3) and subject to the first sale doctrine. The copyright owner in *Quality King* could not invoke section 602(a)(1) to preclude re-importation and sale of products manufactured in the United States (with copyrighted labels and packaging) for sale abroad, which was protected by the first sale doctrine.[9] However, as Justice Ginsburg pointed out, dictum in that opinion specifically noted that if the author of a work had granted exclusive British distribution rights to a publisher of a British edition, "the first sale doctrine would not provide the publisher of the British edition who decided to sell in the American market with a defense."[10]

Kirtsaeng may be one of the most significant copyright decisions by the Supreme Court in recent years, but it deals squarely with old-fashioned books (textbooks, in particular). The Court does not address the dissemination of written content online—sales or lending of e-books, downloading files from websites, or distribution of other kinds of electronic, virtual, or cyberproperty. However, the Court does support its decision in part by noting, with reference to various amici, that finding a geographical limitation within the first sale doctrine (as advocated by Wiley) would fail to further the Copyright Act's essential purpose in "promot[ing] the progress of Science and useful Arts."[11] Among other things, it could restrict the distribution of books printed abroad by libraries and booksellers, and it could impact the resale in the United States of automobiles, computers, and many kinds of consumer electronic devices initially sold overseas, which contain copyrighted software or packaging.[12]

5. *Kirtsaeng*, 133 S. Ct. at 1356.
6. *Id.*
7. *Id.* at 1358.
8. 523 U.S. 135 (1998).
9. *Kirtsaeng*, 133 S. Ct. at 1375 (quoting *Quality King*, 523 U.S. at 143–54).
10. *Id.* (quoting *Quality King*, 523 U.S. at 148).
11. *Id.* at 1364 (internal quotation omitted).
12. *Id.* at 1364–65.

Republication of Digital or Online Content: Will the First Sale Doctrine or Any Other Copyright Exception Apply?

Despite the apparent expansive view of the majority in *Kirtsaeng*, its impact on the scope of the first sale doctrine may be somewhat limited when applied to other copyrighted content. For example, a software licensee may not invoke the first sale doctrine to protect modification of that software in a new product, as affirmed by a federal district court ruling last year.[13]

Could the first sale doctrine protect the redistribution of copyrighted content posted to a webiste? For example, after photographs have been posted to an internet service like Twitter, may others republish them? In *Agence France Presse v. Morel*,[14] the court considered whether a news agency (AFP) infringed a photojournalist's copyright through its republication of photographs uploaded to Twitter through the TwitPic application. The court determined that the Twitter and TwitPic terms of service do not provide an express license to non-partner third parties such as AFP to republish photos posted to TwitPic.[15] AFP then pursued a theory that it was a third-party beneficiary of the Twitter and TwitPick terms of service, but the court rejected that argument and granted plaintiff's motion for summary judgment that AFP and co-defendant *The Washington Post* were liable for copyright infringement.[16]

If the first sale doctrine protects resale of hard copy versions of a published musical work, such as a chart or sheet music, why not a digital file of a song? That was the defendant's approach in *Capitol Records, LLC v. ReDigi Inc.*,[17] whose service allowed people to upload digital songs and then sell them to others at a discount from the price they had paid to acquire the songs from the Apple iTunes service.

ReDigi argues that the first sale defense protected these resales of digital song files. The court pointed out that the first sale doctrine would potentially protect only the *distribution* of a copyrighted work, not a *reproduction* of the work, and ReDigi users would have to create new copies of a song when they sought to resell them on the service.[18] In other words, although the user had lawfully obtained a copy of the song by downloading it from iTunes, the court found the first sale doctrine not to apply because a user would necessarily have to create

13. *See* Adobe Sys., Inc. v. Hoops Enter. LLC, No. C 10-2769 CW, 2012 WL 298732 (N.D. Cal. Feb. 1, 2012) (granting partial summary judgment to plaintiff and finding that first sale doctrine does not apply to sale of Adobe software unbundled from the hardware with which it was originally sold). This ruling follows Ninth Circuit decisions in *Vernor v. Autodesk*, 612 F.3d 1102, 1106–07 (9th Cir. 2010) (licensee is not an owner of a particular copy under 17 U.S.C. § 109(a) and thus the first sale doctrine does not apply to redistribution of a work), *cert. denied*, 132 S. Ct. 105 (2011) and *Apple v. Psystar Corp.*, 658 F.3d 1150 (9th Cir. 2011).

14. 769 F. Supp. 2d 295 (S.D.N.Y. 2011).

15. *Id.* at 302–03.

16. AFP v. Morel, No. 10 Civ. 02730-AJN, 2013 WL 146035 (S.D.N.Y. Jan. 14, 2013). The case is proceeding to trial on damages. *See* AFP v. Morel, No. 10 Civ. 02730-AJN, 2013 WL 2253965 (S.D.N.Y. May 21, 2013).

17. No. 12 Civ. 95 (RJS), 2013 WL 1286134 (S.D.N.Y. Mar. 30, 2013).

18. *Id.* at *12.

a new copy, i.e., make a reproduction of the copyrighted work, in violation of the reproduction right, in order to resell it.[19]

Do websites necessarily infringe copyrights by reposting articles in new online formats? Stated differently, might reposting of news stories, whether because of the service provided to users or the manner in which the stories are posted, qualify as fair use? In March, the U.S. District Court for the Southern District of New York rejected the defenses of an online news aggregator website in a copyright infringement action brought by the Associated Press.[20] The defendant, Meltwater News, uses software to scrape news articles from other websites and to download content to its servers for searching by customers on its own subscription-based aggregated news report service.[21] Meltwater asserted that reposting excerpts of articles from the Associated Press constituted a fair use and that it had an implied license to do so.[22] Meltwater's fair use defense was based on the assertion that it functions as an internet search engine and provides limited amounts of copyrighted material to its users according to their queries.[23]

The court did not accept Meltwater's self-characterization that its service was more akin to a search engine, but instead viewed it as a subscription news service that markets itself as a news clipping service.[24] Based in large part on this characterization and on the finding that click-through rates to the full articles in question were relatively low (meaning that the service did not operate to help consumers reach the underlying news sources but instead served as a substitute), the court found that the service was not "transformative," one of the factors in determining fair use.[25] After analyzing the other fair use factors and finding that defendant failed to meet them, including noting that the defendant's business was based on competing directly with the copyright owner, the defense failed.[26] Meltwater also claimed an implied license to republish the articles because AP licensees that published them on their sites made no effort to preclude webcrawlers like those used by the Meltwater service from scraping the sites and copying the content.[27] The court found, however, that no such implied license could arise in the absence of a fair use.[28]

19. *Id.* at *11–12.

20. Associated Press v. Meltwater News U.S. Inc., No. 12 Civ. 1087 (DLC), 2013 WL 1153979 (S.D.N.Y. Mar. 21, 2013).

21. *Id.* at *11–12.

22. *Id.* at *26, *57.

23. *Id.* at *26.

24. *Id.* at *33–34.

25. *Id.* at *36–37, *44–45

26. *See id.* at *41–42. The court distinguished two earlier significant internet copyright cases from the Ninth Circuit, *Perfect 10 v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007) (vacating preliminary injunction and finding co-defendant Google likely to prevail in showing fair use defense in reposting of Perfect 10's photos as thumbnails in search engine results) and *Kelly v. Arriba Soft Corp.*, 336 F.3d 811 (9th Cir. 2003) (holding display of thumbnails in search engine results was fair use).

27. *Associated Press*, 2013 WL 1153979, at *60–61.

28. *Id.* at *23–24.

More from the Nonpracticing IP Plaintiffs

Last year's survey covered some of the difficulties several courts faced when dealing with the aggressive tactics of copyright litigants seeking the identification of John Doe respondents charged with illegal downloading of copyrighted content.[29] This year, it seemed some courts are becoming less tolerant of many of these plaintiffs' tactics. Using intellectual property rights as a means to create a revenue stream without any active business operation is not new, but recently courts are taking notice of aggressive and potentially unwarranted litigation tactics involving copyright strategies.

In an opinion from the Ninth Circuit involving the frequent copyright litigant Righthaven LLC,[30] the court affirmed a dismissal for lack of standing in two copyright infringement lawsuits. The court affirmed the finding that the plaintiff had no standing despite Righthaven's assertion that it obtained the right to sue for infringement from contracts purportedly granting that right without a transfer of any actual exclusive rights in the copyrighted works, thus undermining the foundation of Righthaven's litigation strategy.[31]

Righthaven had filed separate copyright infringement lawsuits against two defendants[32] for posting online two newspaper articles without permission.[33] The *Las Vegas Review-Journal*, owned by Stephens Media, LLC, held the copyrights in the two articles.[34] Stephens Media entered into both a copyright assignment agreement and a strategic alliance agreement with respect to each copyrighted article, purporting to give Righthaven the right to pursue infringers.[35] The court affirmed the district court's finding that, since the agreements gave only the right to sue for infringement but did not grant any other exclusive rights under the Copyright Act to Righthaven, there was an insufficient transfer of rights to confer standing.[36] It remains to be seen whether Righthaven will adjust the structure of its alliance agreements in subsequent relationships, so it may continue its practice of finding infringement lawsuits to assert.

Meanwhile, another active copyright litigant, Prenda Law, Inc., recently found itself subject to an order for sanctions in the United States District Court for the Central District of California.[37] The court found that certain individuals related to the plaintiffs in copyright infringement claims were attorneys who had conspired to operate a joint enterprise, forming certain legal entities with the sole

29. *See* Dorrain & Rubens, *supra* note 1, at 317–18.

30. Righthaven, LLC v. Hoen, 716 F.3d 1166 (9th Cir. 2013).

31. *Id.* at 1171–72.

32. Defendant Wayne Hoehn had posted a newspaper article to the comments section of a sports website he followed; defendant Thomas Biaise posted a different article to his blog; the two cases were consolidated on appeal.

33. *Id.* at 1168.

34. *Id.*

35. *Id.* at 1169–72.

36. *Id.*

37. Ingenuity 13 LLC v. John Doe, No. 2:12-CV-8333-ODW (JCx), 2013 WL 1898633 (C.D. Cal. May 6, 2013) (order issuing sanctions). The plaintiff Ingenuity 13 was found to be an entity related to other entities that had participated in this and other similar litigation, including AF Holdings, LLC and Prenda Law, Inc. *Id.* at *4.

purpose of litigating copyright infringement lawsuits.[38] These entities obtained copyrights to pornographic movies and then monitored BitTorrent download activity and recorded IP addresses associated with those downloads.[39] They filed lawsuits in federal district court seeking to subpoena internet service providers for the identities of persons associated with those IP addresses and then sent cease-and-desist letters with monetary settlement offers to those persons.[40]

In one of the most assertive rebukes yet to the tactics employed by this group of litigants, the court issued an order finding that lawyers involved had engaged in vexatious litigation designed to coerce settlement, submitted misinformation to the court, and made misrepresentations to the court concerning the nature of their associations and operations as well as the extent of their investigations concerning whether a download had actually been completed by the owner of the IP address.[41] The court issued sanctions under its inherent authority to sanction misconduct, awarding doubled attorney's fees and costs to the Doe defendants.[42]

These proceedings go on, but this order may be an indication that the courts will have less tolerance in the future for similar aggressive tactics from litigants obtaining rights in copyrights in order to force settlements from downloaders.

38. *Id.*
39. *Id.*
40. *Id.*
41. *Id.* at *4, *6–7.
42. *Id.* at *10.

The Changing Scope of Patent Rights

*By Phong D. Nguyen**

Introduction

Over the past year, the Federal Circuit has decided a number of patent cases covering different phases of infringement proceedings. In *InterDigital Communications, LLC v. ITC*, the court addressed whether the International Trade Commission ("ITC") has jurisdiction to enforce the patent rights of non-practicing entities, i.e., parties that neither develop nor market patented articles but engage only in licensing activities. The court also issued its much-awaited decision concerning the patent eligibility of computer-related methods and systems in *CLS Bank International v. Alice Corp.* In *Akamai Technologies, Inc. v. Limelight Networks, Inc.*, the court addressed a potential loophole within the "single entity rule" for induced infringement. Finally, *LaserDynamics, Inc. v. Quanta Computer, Inc.* provides a useful framework for properly determining the reasonable royalty in a case of active infringement.

InterDigital Communications, LLC v. ITC—Non-Practicing Entities Continue to Have Jurisdiction in the ITC

On January 10, 2013, the Federal Circuit denied a petition for rehearing filed by Nokia Inc. ("Nokia") and affirmed its decision that a non-practicing entity's patent licensing activities satisfy the "domestic industry" requirement of section 337 of the Tariff Act of 1930, as amended.[1] This decision upheld the ITC's jurisdiction in enforcing patent rights for non-practicing entities.[2]

A primary purpose of the ITC has been to protect U.S. industry from "unfair" foreign competition.[3] Under section 337 of the Tariff Act of 1930,[4] a party wishing to enforce patents through the ITC must satisfy a "domestic industry"

* Phong D. Nguyen is a partner with Baker Hostetler LLP in its D.C. Office where he practices client counseling, patent portfolio management and procurement, and patent litigation. The author thanks Kevin Y. Liu and Chinenye Okafor, summer associates at Baker Hostetler LLP, for their work in researching, summarizing the cases, and editing this survey.

1. InterDigital Commc'ns, LLC v. ITC, 707 F.3d 1295, 1297 (Fed. Cir. 2013) (interpreting 19 U.S.C. § 1337), *cert. denied*, 81 U.S.L.W. 3652 (U.S. Oct. 15, 2013) (No. 12-1352).
2. *Id.* at 1304.
3. *See id.*
4. 19 U.S.C § 1337 (2012).

requirement.[5] This requirement is satisfied by any of the following: "(A) significant investment in plant and equipment; (B) significant employment of labor or capital; or (C) substantial investment in [the patent's] exploitation, including engineering, research and development, or licensing."[6]

InterDigital Communications, LLC ("InterDigital") filed a complaint with the ITC against Nokia for infringement of two patents directed to wireless cellphone CDMA technology.[7] The administrative judge found no infringement based on a narrow claim construction.[8] On appeal, the Federal Circuit construed the claims more broadly and found that Nokia's activities infringed InterDigital's patents.[9]

Nokia petitioned the Federal Circuit for a panel rehearing as well as a rehearing en banc and argued that InterDigital did not satisfy the "domestic industry" requirement.[10] Nokia argued that the ITC and the Federal Circuit panel misconstrued the statutory language "relating to the articles protected by the patent" in section 337(a)(2) and "with respect to the articles protected by the patent" in section 337(a)(3).[11] Nokia contended that this statutory language meant that the only licensing activity that matters, for purposes of establishing "domestic industry," is activity "with respect to the articles protected by the patent."[12] Nokia further argued that this licensing activity must be tethered to a tangible good and that the technology covered by the patent must be put into practical use.[13]

In denying Nokia's petition, the Federal Circuit explained that domestic licensing activity is sufficient to satisfy standing requirements before the ITC.[14] According to the majority, the legislative intent was to offer relief under section 337 to a party that has made a substantial investment in exploitation of a patent through engineering, research and development, or licensing.[15] Thus, it is not necessary that the patentee or even any other domestic party manufacture the patented product.[16] As long as the patent covers the article and a party seeking relief can show that it has a sufficiently substantial investment, including an investment in licensing, that party is entitled to seek relief under section 337.[17]

The key phrase in the Federal Circuit's analysis of section 337 is "substantial investment."[18] In this case, InterDigital invested a total of approximately $7.6 million in salaries and benefits for employees engaged in its licensing activ-

5. *Id.* § 1337(a)(2)–(3).
6. *Id.* § 1337(a)(3)(A)–(C).
7. InterDigital Commc'ns, LLC v. ITC, 690 F.3d 1318, 1323 (Fed. Cir. 2012), *petition for rehearing denied*, 707 F.3d 1295 (Fed. Cir. 2013), *cert. denied*, 81 U.S.L.W. 3652 (U.S. Oct. 15, 2013) (No. 12-1352).
8. *Id.* at 1323–24.
9. *See id.* at 1330.
10. *InterDigital Commc'ns*, 707 F.3d at 1297 (citing 19 U.S.C. § 1337(a)(3) ("an industry in the United States")).
11. *Id.*
12. *Id.* at 1299.
13. *Id.*
14. *See id.* at 1300.
15. *Id.* at 1303.
16. *Id.* at 1304.
17. *Id.*
18. *Id.*

ities, had twenty-four revenue producing licensees, and received almost $1 billion in revenues from portfolio licenses.[19] The Federal Circuit found that this constituted "substantial investment."[20] This decision raises a line-drawing problem in determining a "substantial investment" necessary to satisfy the "domestic industry" requirement. Moreover, in a dissent that challenged the majority's construction of section 337, Judge Newman argued that Congress intended for section 337 to support domestic production, not mere licensing.[21] Although the Supreme Court denied Nokia's petition for certiorari,[22] the division of opinion within the Federal Circuit suggests the potential for future refinement of these jurisdictional questions.

CLS Bank International v. Alice Corp.—Is Software Patent Eligible?

The en banc decision in *CLS Bank International v. Alice Corp.*[23] was highly anticipated to resolve questions surrounding the patent eligibility of computer implemented method and system claims.[24] A majority of the ten-judge panel ruled that the asserted method claims were ineligible, while an equally divided court affirmed the ineligibility of the system claims.[25] Because a majority could not agree on the reasoning, the decision unfortunately does not resolve questions of how patent eligibility will be determined in the future.[26]

Alice Corporation ("Alice") owned several patents relating to a computerized trading platform used to eliminate counterparty or settlement risks by having a third party guarantee obligations related to a financial transaction between the first and second parties.[27] For example, if two parties entered into an agreement, there may be a period of time after the agreement but before the actual execution of the agreed upon trade, where one party might become unable to pay and neglect to notify the other party prior to settlement.[28] Alice allocated this risk to a third party that would verify each party's ability to perform and guarantee the exchange obligations.[29]

In May 2007, CLS Bank International ("CLS") sought a declaratory judgment of non-infringement, invalidity, and unenforceability as to Alice's patents, claiming the patents were not directed to patent-eligible subject matter.[30] Section 101 of Title 35 of the United States Code states that "[w]hoever invents or discovers

19. *Id.* at 1299.
20. *Id.*
21. *See id.* at 1304–05 (Newman, J., dissenting).
22. Nokia Inc. v. ITC, 81 U.S.L.W. 3652 (U.S. Oct. 15, 2013) (No. 12-1352).
23. 717 F.3d 1269 (Fed. Cir. 2013) (en banc).
24. *See* 35 U.S.C. § 101 (2012) ("Inventions patentable").
25. *CLS Bank Int'l*, 717 F.3d at 1273 (per curiam). Judge Taranto did not participate in the decision. *Id.* at 1273 n.*.
26. *See id.* at 1270, 1273.
27. *Id.* at 1274 (Lourie, J., concurring).
28. *Id.*
29. *Id.*
30. *See id.*

any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title."[31] CLS argued that the claims were drawn to cover ineligible subject matter.[32]

Previously, the district court had sided with CLS and agreed that the claims were "directed to an abstract idea of employing an intermediary to facilitate simultaneous exchange of obligations in order to minimize risk."[33] A panel of the Federal Circuit reversed the district court and found the claims to be eligible subject matter.[34] However, after agreeing to hear the issue en banc, the Federal Circuit generated seven opinions that outline three different views on patent eligibility, none of which garnered majority support.[35]

Judge Lourie, joined by Judges Dyk, Prost, Reyna, and Wallach, articulated one standard for determining patent eligibility.[36] Judge Lourie stated that, once a section 101 exception applies (i.e., "laws of nature, natural phenomena, and abstract idea"[37]), the abstract idea or law of nature must be isolated from the underlying claim.[38] The analysis should then turn to whether a claim adds "significantly more" or an "inventive" step to the abstract idea or law of nature.[39] The claim should contain additional substantive limitations that narrow the claim so that the claim does not, for practical purposes, cover the full abstract idea itself.[40]

Applying this analysis to the facts of the case, Judge Lourie determined that the abstract idea at issue is "reducing settlement risk by facilitating a trade through third-party intermediation"; thus, the computer-readable limitations added nothing of substance to the claims.[41] Because there was nothing added to this abstract idea, he then concluded that neither the method claims nor the system claims were patent eligible.[42]

Chief Judge Rader, joined by Judges Linn, Moore, and O'Malley, articulated a different standard for determining eligibility.[43] Chief Judge Rader reasoned that the whole claim must be evaluated without separating the claim from the

31. 35 U.S.C. § 101 (2012).
32. *CLS Bank Int'l*, 717 F.3d at 1275 (Lourie, J., concurring).
33. *Id.*
34. CLS Bank Int'l v. Alice Corp., 685 F.3d 1341, 1343 (Fed. Cir. 2012), *aff'd*, 717 F.3d 1269 (Fed. Cir. 2013) (en banc).
35. *See CLS Bank Int'l*, 717 F.3d at 1273 (per curiam); *id.* (Lourie, J., concurring); *id.* at 1292 (Rader, C.J., concurring in part and dissenting in part); *id.* at 1313 (Moore, J., dissenting in part); *id.* at 1321 (Newman, J., concurring in part and dissenting in part); *id.* at 1327 (Linn & O'Malley, JJ., dissenting). At the end of the opinion, Chief Judge Rader also offered "[a]dditional reflections." *Id.* at 1333.
36. *Id.* at 1273 (Lourie, J., concurring).
37. *Id.* at 1277 (quoting Diamond v. Diehr, 450 U.S. 175, 185 (1981)).
38. *See id.* at 1282.
39. *Id.* at 1280, 1282 (citing Mayo Collaborative Servs. v. Prometheus Labs., Inc., 132 S. Ct. 1289, 1294–98 (2012)).
40. *Id.* at 1281 (citing *Mayo*, 132 S. Ct. at 1294, 1302).
41. *Id.*
42. *Id.* at 1292.
43. *Id.* (Rader, C.J., concurring in part and dissenting in part).

abstract idea.[44] An abstract idea may only be claimed if the claim includes "meaningful limitations" that restrict the idea to a specific application.[45] "Meaningful limitations" are those limitations essential to the invention that do "more than recite pre- or post-solution activity" and are "central to the solution itself."[46] "At bottom, where the claim is tied to a computer in such a way that the computer plays a meaningful role in the performance of the claimed invention, and the claim does not pre-empt virtually all uses of an underlying abstract idea, the claim is patent eligible."[47]

With this approach, Chief Judge Rader found that the system claims were patent eligible. For the system claims, Chief Judge Rader noted that the claimed data processing system had a number of limitations that narrowed the preemptive effect.[48] The system claims included at least four separate structural components and at least thirty-two figures, which provided detailed algorithms for the software with which this hardware was to be programmed.[49] With these limitations, Judge Rader found that the abstract idea was properly embodied and integrated into a system using machines.[50]

However, using the same approach, Chief Judge Rader found that the method claims were patent ineligible.[51] Each step of the method claim recited a general step inherent within the concept of an escrow, using a third-party intermediary.[52] None of the steps recited use of a computer to facilitate the transactions.[53] Thus, the claims were ineligible because they added nothing beyond the well-known procedures used in the concept of an escrow.[54]

Dissenting in part, Judge Moore, joined by Chief Judge Rader and Judges Linn and O'Malley, outlined a third approach to address the subject matter eligibility of computer-related patents.[55] She expressed her grave concern that the current interpretation of section 101 was causing serious problems within the patent system.[56] She criticized the other judges for erroneously applying the "inventive concept" language by first stripping away all known elements and analyzing the remainder, instead of applying the concept to the claim as a whole.[57] To challenge a claim for a well-known concept, Judge Moore believes that the proper avenue is through use of sections 102 and 103.[58]

44. *Id.* at 1298.
45. *Id.* at 1299.
46. *Id.* at 1301.
47. *Id.* at 1302.
48. *Id.* at 1307–11.
49. *Id.* at 1307.
50. *Id.* at 1311.
51. *Id.* at 1312–13.
52. *Id.* at 1311.
53. *Id.* at 1312.
54. *Id.*
55. *See id.* at 1313 (Moore, J., dissenting in part).
56. *See id.* at 1313–14.
57. *Id.* at 1315.
58. *Id.* at 1314–15 (citing 35 U.S.C. §§ 102–103).

Because no approach commanded a majority, the decision in *CLS Bank International* does not effectively address how patent eligibility should be approached in the future. Thus, until the Supreme Court can provide some much needed guidance, the patent eligibility of computer-related claims remains unanswered.

Akamai Technologies, Inc. v. Limelight Networks Inc.—Joint Infringement Standard Relaxed

Recently, the Federal Circuit issued another much anticipated en banc opinion resolving an issue of "joint" infringement. In *BMC Resources, Inc. v. Paymentech, L.P.*, a panel of the Federal Circuit required a single entity to be liable for direct infringement before a second party could be liable for induced infringement.[59] This "single-entity rule" allowed parties to escape liability when no single party performed all of the steps of a patented method.[60] To close this loophole, the Federal Circuit in *Akamai Technologies, Inc. v. Limelight Networks, Inc.*, sitting en banc, expressly overruled *BMC Resources* and announced that it no longer requires a single entity to perform all of the steps of a method claim.[61]

The dispute in *Akamai* involved a method claim for efficient delivery of web content.[62] The method included steps of placing content on a set of replicated servers and then modifying a web page so that web browsers could properly retrieve the content.[63] The defendant, Limelight Networks, Inc. ("Limelight"), managed a system of servers in a manner claimed by the patent; however, Limelight instructed customers on how to modify web pages to receive the web content.[64] Under *BMC Resources*, Limelight would not be liable for induced infringement because no single party performed all of the steps of the claimed method.[65]

A strict application of *BMC Resources* would yield a bizarre result. Normally, when one party knowingly encourages another party to practice all steps of a patent method, the first party is held liable for induced infringement, while the second party is held liable for direct infringement.[66] It would be strange if that first party could escape liability simply by performing one of the steps of a patented method, while encouraging the second party to undertake any remaining steps.[67] A party that actually performs one step of a patent method is, if anything, more culpable than one who does not perform any steps.[68]

In overruling *BMC Resources*, the Federal Circuit reinterpreted section 271(b) of Title 35 of the United States Code,[69] which recites that "[w]hoever actively

59. 498 F.3d 1373, 1379–81 (Fed. Cir. 2007).
60. *Id.* at 1380.
61. 692 F.3d 1301, 1306 (Fed. Cir. 2012) (en banc).
62. *Id.*
63. *Id.*
64. *Id.*
65. *See id.* at 1306–07.
66. *Id.* at 1309.
67. *Id.*
68. *Id.*
69. *Id.* at 1309–14.

induces infringement of a patent shall be liable as an infringer."[70] The court clarified that the term "infringement" in section 271(b) does not refer to the direct infringement outlined in section 271(a), but simply denotes "acts necessary to infringe a patent."[71] In this regard, the court found no limitation that the acts necessary to support induced infringement must have been performed by a single party.[72] Legislative history as well as principles of tort law supported this broader interpretation of inducement liability.[73] With this decision, a party wishing to prove induced infringement must show: (A) the defendant knew of the patent, (B) the defendant induced another to perform one or more of the steps of the method claimed in the patent, (C) those steps were performed, and (D) if the defendant did not induce another to perform all of the steps, then the defendant performed any remaining steps.[74] Consequently, all of the steps of the method claim do not need to be performed by a single entity.[75]

In his dissent, Judge Linn criticized the majority's "inducement-only rule."[76] Under the majority's rationale, the inducer would be found liable, but the induced party that performed only some of the steps of the method claim would not be liable, because that party would not have performed all of the steps.[77] This result may seem reasonable in *Akamai* because the customers did not seem worthy of blame, when they simply acted in accord with Limelight's instructions in performing one step of a patented method.[78] However, this decision could shift culpability away from a more complicit party in the future because that party did not perform all of the steps in a patented method.

LaserDynamics, Inc. v. Quanta Computer, Inc.—Proper Framework for Royalty Calculation

In *LaserDynamics, Inc. v. Quanta Computer, Inc.*, the Federal Circuit clarified the framework for determining a reasonable royalty in a case of patent infringement.[79] The court overturned an $8.5 million jury award and remanded the case for a new determination of damages.[80] The decision addressed issues concerning the "entire market value" rule as well as how to determine the hypothetical negotiation date.[81]

LaserDynamics, Inc. ("LaserDynamics") alleged Quanta Computer, Inc. ("Quanta") committed patent infringement through the sale of laptop computers

70. 35 U.S.C. § 271(b) (2012).
71. *Akamai Techs.*, 692 F.3d at 1309.
72. *Id.*
73. *See id.* at 1310–13.
74. *See id.* at 1318.
75. *Id.*
76. *Id.* at 1337 (Linn, J., dissenting).
77. *Id.* at 1339.
78. *Id.* at 1306 (majority opinion).
79. 694 F.3d 51 (Fed. Cir. 2012).
80. *Id.* at 65, 81–82.
81. *Id.*

that contained LaserDynamics' patented optical disc drive technology.[82] In the first trial, LaserDynamics applied the "entire market value" rule using revenues from sales of laptop computers as the royalty base for its damages calculations, even though the patented technology was limited to the disc drives.[83] After the jury found Quanta liable for infringement, the district court granted Quanta's motion for new trial because the "entire market value" rule was improperly applied.[84] LaserDynamics did not sufficiently demonstrate that the patented technology drove demand for the laptop computers.[85] In the second trial, the jury awarded a lump sum of $8.5 million in damages, which was appealed by both parties to the Federal Circuit.[86]

The Federal Circuit reiterated that the "entire market value" rule is a narrow exception to the general rule that royalties are not based on the value of the entire product, but are instead based on the "smallest salable patent-practicing unit."[87] In order to calculate damages based on the entire product, a patentee must show demand for the entire product is attributable to the patented feature.[88]

LaserDynamics argued that a laptop was not a commercially viable product without an optical disc drive.[89] However, even if LaserDynamics proved that consumers would not buy a laptop without the drive, such proof—according to the court—was not sufficient to show the optical drive drove demand for the product.[90] LaserDynamics had the burden of showing the presence of the optical drive motivated the consumer to buy a laptop in the first place.[91]

The Federal Circuit also discussed setting the proper hypothetical negotiation date for royalty calculations. Normally, the royalties are based on what two willing parties would agree to pay for a license under a hypothetical negotiation from the date that the infringement began.[92] The Federal Circuit deemed the hypothetical negotiation to occur on the first instance of inducing conduct that resulted in direct infringement.[93]

Previously, the district court reasoned that the date of notice was the proper hypothetical negotiation date because that was when Quanta first met all of the elements of induced infringement.[94] The Federal Circuit found error and explained that Quanta's first act of inducing conduct occurred in 2003 when it began selling the accused laptops.[95] Therefore, the Federal Circuit instructed

82. *Id.* at 59.
83. *Id.* at 63.
84. *Id.*
85. *Id.*
86. *Id.* at 65.
87. *Id.* at 67 (quoting Cornell Univ. v. Hewlett-Packard Co., 609 F. Supp. 2d 279, 283, 287–88 (N.D.N.Y. 2009)).
88. *Id.* at 67–68.
89. *Id.* at 68.
90. *Id.*
91. *Id.*
92. *Id.* at 75.
93. *Id.* at 76.
94. *See id.* at 75.
95. *Id.* at 75–76.

that, on remand, the hypothetical negotiation analysis should be based on a 2003 date.[96] An earlier hypothetical negotiation date favored LaserDynamics because it would receive royalties beginning from the earlier date.

The Federal Circuit also addressed the use of litigation settlement agreements as evidence for establishing a reasonable royalty. The Federal Circuit noted that the "propriety of using prior settlement agreements to prove the amount of a reasonable royalty is questionable."[97] The court reasoned that the coercive environment of patent litigation does not accurately reflect the proper standard of a voluntary agreement reached between a willing licensee and licensor.[98]

The Federal Circuit concluded that the district court abused its discretion by admitting into evidence the 2006 litigation settlement agreement between LaserDynamics and BenQ Corporation ("BenQ"), an alleged infringer.[99] BenQ agreed to the settlement shortly before trial after it had been "repeatedly sanctioned . . . for discovery misconduct and misrepresentation."[100] Further, BenQ settled for an amount several times larger than the amount due under any of the other licenses admitted into evidence.[101] The court ruled that the agreement should not have been admitted into evidence.[102]

Conclusion

The Federal Circuit has answered several questions concerning the various stages of a patent infringement proceeding. The court found that the ITC has jurisdiction to enforce the patent rights of non-practicing entities because licensing activities are enough to satisfy the "domestic industry" requirement. However, the decision may lose relevance as President Obama recently issued several executive actions to curb the abundance of lawsuits by non-practicing entities.[103] Furthermore, a party no longer needs to show a single entity performed all elements of a claimed method in order to find induced infringement, which eliminates a potential loophole in the law. In terms of reasonable royalty calculations, a party must show customers bought a product because of the patented component before relying on the entire market rule, while the proper date for calculating a royalty begins with the first instance of inducing conduct. Unfortunately, the eligibility of computer-related patent claims still remains dubious, as the Federal Circuit was not able to reach a consensus on the proper standard to apply. Hopefully, this important issue will be addressed by the Supreme Court in the near future.

96. *Id.* at 76–77.
97. *Id.* at 77.
98. *Id.*
99. *Id.* at 58, 78.
100. *Id.* at 58.
101. *Id.* at 78.
102. *Id.*
103. Press Release, The White House, Fact Sheet: White House Task Force on High-Tech Patent Issues (June 4, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/06/04/fact-sheet-white-house-task-force-high-tech-patent-issues.

The Shifting Tide in Internet Gambling—Survey of Recent Developments

*By Kenneth N. Caldwell**

Introduction

Internet gambling in the United States is picking up steam. In 2011, the Department of Justice ("DOJ") opined that language in the 1961 Wire Act that criminalized certain activities related to the "placing of bets or wagers on any sporting event or contest"[1] did not also encompass "non-sporting events" within its scope.[2] The direct result of the DOJ's thirteen-page opinion ("DOJ Opinion") was to green-light proposals by Illinois and New York to proceed with in-state lotteries that rely on the interstate transmission of data to serve their in-state customers.[3] The indirect effect of the DOJ Opinion was to green-light internet gambling for "non-sporting events," particularly online poker, which, for the most part, had been banished due to the uncertainty of criminal prosecution under previous interpretations of the Wire Act.[4]

The DOJ Opinion, along with the enactment of gambling- and/or poker-friendly legislation in states such as Delaware, Nevada, and New Jersey, have reinvigorated internet poker, and to some extent a broader spectrum of gambling in the United States. Several international-based internet companies that previously departed the U.S. market in fear of the Unlawful Internet Gambling Enforcement Act of 2006 ("UIGEA")[5] have renewed their interest and are making

* Kenneth N. Caldwell is a Shareholder in McDowell Rice Smith & Buchanan, P.C. in Kansas City, Missouri. Mr. Caldwell has been licensed in Nevada since 1989 and has also served as in-house general counsel to a company in the State of Delaware.

1. 18 U.S.C. § 1084(a) (2012).

2. Whether Proposals by Illinois and New York to Use the Internet and Out-of-State Transaction Processors to Sell Lottery Tickets to In-State Adults Violate the Wire Act, 35 Op. O.L.C. 1 (Sept. 20, 2011) [hereinafter DOJ Opinion], *available at* http://www.justice.gov/olc/2011/state-lotteries-opinion.pdf.

3. *Id.* at 1–2.

4. *See* United States v. Lombardo, 639 F. Supp. 2d 1271, 1277–82 (D. Utah 2007) (rejecting, years before the issuance of the DOJ Opinion, defendant's argument that the Wire Act prohibited only sports-based wagers, not casino-like gambling); DOJ Opinion, *supra* note 2, at 2 (noting that, historically, the Criminal Division of the DOJ had uniformly taken the position that the Wire Act prohibited non-sporting event, interstate gambling).

5. 31 U.S.C. §§ 5361–5367 (2012).

new investments in the U.S. market.[6] Before the issuance of the DOJ Opinion, UIGEA severely restricted companies headquartered outside of the United States from receiving funds from players in the United States because it criminalized the receipt of funds from "unlawful Internet gambling,"[7] and internet gambling had been long considered "unlawful" under the Wire Act.[8] No longer to be used as a sword by the government, the ambiguity in the Wire Act has now been clarified, the floodgates have been lifted, and many of the market participants are now jockeying for position in the new legal landscape without fear of prosecution.

Department of Justice Opinion

Given that the Wire Act was enacted in 1961,[9] it was somewhat surprising when some fifty years later, on December 23, 2011, the DOJ released its opinion restricting the scope of the Act's criminal proscriptions.[10] The DOJ Opinion responded to a combined request from New York and Illinois regarding lottery proposals that involved the use of the internet and out-of-state processors in the sale of in-state lottery tickets.[11] The long overdue opinion stated that "interstate transmissions of wire communications that do not relate to a 'sporting event or contest' . . . fall outside of the reach of the Wire Act."[12]

The issue was brought to a head, perhaps strategically, because New York announced that it intended to implement a new computerized system to manage the sale of lottery tickets to in-state customers. Specifically, New York proposed that, in addition to the traditional tickets purchased over the counter at brick-and- mortar establishments in New York, it should also be allowed to deliver virtual tickets electronically over the internet to customers' mobile phones and computers located inside New York.[13] The proposed system, however, would route transaction data to data centers in New York and Texas through networks controlled in Maryland and Nevada.[14] Similarly, Illinois intended to route packets of data over the internet (and impliedly across state lines) even though its lottery ticket sales were to be restricted to Illinois residents using geolocation

6. *See* Nathalie Thomas, *Online Gaming Companies Return to U.S. Markets*, Telegraph (Feb. 27, 2013, 7:49 PM), http://www.telegraph.co.uk/finance/newsbysector/retailandconsumer/leisure/9898656/Online-gaming-companies-return-to-US-market.html.

7. 31 U.S.C. § 5363.

8. *See* DOJ Opinion, *supra* note 2, at 1–2.

9. Pub. L. No. 87-216, 75 Stat. 491 (1961) (codified as amended at 18 U.S.C. § 1084 (2012)).

10. Karoun Demirjan, *DOJ Opinion 'Important Day' in Efforts to Legalize Online Gaming*, Las Vegas Sun (Dec. 23, 2011, 7:21 PM), http://www.lasvegassun.com/news/2011/dec/23/doj-opinion-important-day-efforts-legalize-online-/#ixzz2PXJtOwRL.

11. *See* DOJ Opinion, *supra* note 2, at 1–2.

12. *Id.* at 1. The DOJ Opinion came too late for Anurag Dikshit, who, in 2008, pleaded guilty to violating the Wire Act, personally forfeited $300 million, and was sentenced to one year of probation. Nathan Vardi, *Convicted Former Online Poker Billionaire Avoids Jail*, Forbes (Dec. 16, 2010, 5:53 PM), http://www.forbes.com/sites/nathanvardi/2010/12/16/convicted-former-online-poker-billionaire-avoids-jail/.

13. DOJ Opinion, *supra* note 2, at 2.

14. *Id.*

technology.[15] The lottery configurations, as proposed by New York and Illinois, were seemingly allowable under UIGEA as "legal Internet gambling," but contrary to previous conflicting court interpretations of the Wire Act, and thus arguably worthy of renewed analysis by the DOJ.[16]

The relevant language in UIGEA prohibits any person engaged in the business of betting or wagering from accepting any credit or funds from another person in connection with the latter person's participation in "unlawful Internet gambling,"[17] a term defined to mean "to place, receive or otherwise knowingly transmit a bet or wager by any means which involves the use, at least in part, of the Internet where such bet or wager is unlawful under any applicable Federal or State law in the State or Tribal lands in which the bet or wager is initiated, received, or otherwise made."[18] Importantly, UIGEA further provides that "unlawful Internet gambling" does not include any "bet or wager . . . initiated and received or otherwise made exclusively within a single State,"[19] and also explains that "[t]he intermediate routing of electronic data shall not determine the location or locations in which a bet or wager is initiated, received, or otherwise made."[20] This limitation involving intermediate routing is critical; if the intermediate routing of electronic data determined the location or locations in which a bet or wager is initiated, received, or made, then the proposed lottery configurations in New York and Illinois could have constituted "unlawful Internet gambling" under UIGEA.[21]

Previously, the DOJ had steadfastly taken the position that the Wire Act prevented internet gambling because it involved a "transmission in interstate . . . commerce of bets or wagers,"[22] but the DOJ Opinion amounted to a surprising about-face.[23] The DOJ Opinion concluded that the phrase "sporting event or contest" as contained in the Wire Act was not meant to include "non-sporting" activities and specifically did not apply to lotteries.[24] Not only did this opinion open the door to the lottery programs proposed by New York and Illinois, it also broadened the scope of what is considered lawful internet gambling, which will now include internet poker and other forms of non-sports betting for which betting establishments can lawfully receive funds from U.S. bettors under UIGEA.

15. *Id.*

16. *Compare In re* Mastercard Int'l, Inc., Internet Gambling Litig., 132 F. Supp. 2d 468, 480 (E.D. La. 2001) ("[A] plain reading of the statutory language clearly requires that the object of the gambling be a sporting event or contest."), *aff'd*, 313 F.3d 257 (5th Cir. 2002), *with* United States v. Lombardo, 639 F. Supp. 2d 1271, 1281 (D. Utah 2007) (concluding that the Wire Act is "not confined entirely to wire communications related to sports betting or wagering").

17. 31 U.S.C. § 5363 (2012).

18. *Id.* § 5362(10)(A).

19. *Id.* § 5362(10)(B)(i).

20. *Id.* § 5362(10)(E).

21. *See id.*; *id.* § 5363.

22. 18 U.S.C. § 1084 (2012).

23. Nathan Vardi, *Department of Justice Flip-Flops on Internet Gambling*, FORBES (Dec. 23, 2011, 3:56 PM), http://www.forbes.com/sites/nathanvardi/2011/12/23/department-of-justice-flip-flops-on-internet-gambling/.

24. *See* DOJ Opinion, *supra* note 2, at 13.

States Jump on the Bandwagon

After the DOJ Opinion was issued, it was only a matter of time before certain gaming-friendly states moved forward with their internet gambling initiatives. Although Nevada had anticipated what it termed "interactive gaming" with earlier legislation and was ahead of the field, Delaware—the first state to ratify the Constitution[25]—was also the first state to act upon the DOJ Opinion by expanding internet gambling opportunities.

A. Delaware

On June 28, 2012, Delaware Governor Jack Markell signed into law the Delaware Gaming Competiveness Act of 2012 ("DGCA").[26] Although Nevada had already conditionally approved "interactive gaming" subject to federal guidance and pre-approval,[27] Delaware was the first state to embrace fully online gambling beyond just poker. The DGCA requires a licensee to verify that a player is in fact located in the state at the time a wager is placed on any game.[28] Such a geographical requirement is quite limiting for a state with a small population. However, an expanded market may be possible, as the legislation also allows "interstate compacts" to the extent that they are "not inconsistent with federal law."[29] The details of the "interstate compacts" are yet to be negotiated, but due to the limited population of the State of Delaware, compacts will likely be necessary to make internet gambling a profitable venture in Delaware.

B. Nevada

On June 10, 2011, before the issuance of the DOJ Opinion, Nevada enacted legislation authorizing the Nevada Gaming Commission ("NGC") to adopt regulations for "interactive gaming," without any specific focus on internet poker.[30] At the same time, the definition of "interactive gaming" was modified to include "Internet poker."[31] Given the uncertainties at that time about the federal policy toward internet poker, Nevada cleverly inserted express conditions in the statute that conditioned the effective date of any license granted under the statute upon the occurrence of either (1) a federal law authorizing interactive gaming or (2) written notification from the DOJ to either NGC or the Nevada Gaming Control Board ("NGCB") that the specific type of interactive gaming anticipated by the license is permissible under federal law.[32]

25. *See* E. Norman Veasey, *What Would Madison Think? The Irony of the Twists and Turns of Federalism*, 34 Del. J. Corp. L. 35, 38 (2009).

26. 2012 Del. Legis. Serv. ch. 285 (West) (H.R. 333) (codified in scattered sections of Del. Code Ann. tit. 29).

27. *See* Nev. Rev. Stat. Ann. § 463.016425(1)(a) (West 2012).

28. *See* Del. Code Ann. tit. 29, § 4826(b) (Supp. 2012).

29. *See id.*

30. *See* Nev. Rev. Stat. Ann. § 463.750 (West 2012).

31. *See id.* § 463.016425(1)(a) ("'Interactive gaming' . . . includes, without limitation, Internet poker.").

32. *See id.* § 463.750(2)(h).

The DOJ Opinion, which arguably satisfied those conditions established by Nevada in 2011, prompted Nevada, during the 2013 legislative session, to authorize internet poker. Seeking specifically to become an internet hub for online poker, the NGCB drafted Assembly Bill No. 114,[33] which was one of the first bills considered during the 2013 legislative session, and which was signed into law on February 21, 2013.[34]

The law allows a broad spectrum of "interactive gaming," but, for economic and political reasons, the NGC has focused on, and drafted regulations for, poker only.[35] The next step in developing internet poker is to expand the potential pool of legal players by entering into compacts with other states. The 2013 Nevada legislation specifically allows the Governor to "enter into agreements with other states, or authorized agencies thereof" to allow players in signatory states to participate in interactive gaming offered by licensees in the other signatory states.[36] The NGC is tasked with coming up with a proposal for interstate compact terms.[37] In an unusual display of urgency, on March 14, 2013, the NGC solicited public comments regarding the terms that should be included in any compact.[38] The following questions were posted on the NGC's website seeking responses from licensees and other interested parties:

1. What topics should the Board and Commission consider putting in regulation relating to an interstate agreement on interactive gaming?
2. Should revenue sharing between signatory states to a compact be based on the location of where the wager originated? Why or why not? Please be specific and cite any relevant legal support.
3. Should revenue sharing between signatory states to a compact be based on the location of the licensed interactive host? Why or why not? Please be specific and cite any relevant legal support.
4. Should the regulatory body of the signatory state where the wager originated have control over player disputes related to said players? Why or why not? Please be specific and cite any relevant legal support.
5. Please provide any other information not requested above that is relevant to regulations for interstate agreements on interactive gaming.[39]

33. *See* 2013 Nev. Legis. Serv. ch. 2 (West) (A.B. 114) (to be codified in scattered sections of NEV. REV. STAT. ANN. ch. 463).

34. *See* Anjeanette Damon & Andrew Doughman, *Nevada Legislature Unanimously Passes Online Poker Bill*, LAS VEGAS SUN (Feb. 21, 2013, 4:12 PM), http://www.lasvegassun.com/news/2013/feb/21/online-poker-bill-moves-forward-nevada-legislature/#ixzz2TDSKuA8o.

35. *See* Anjeanette Damon, *It's Poker Only for Online Gambling in Nevada, for Now*, LAS VEGAS SUN (Mar. 3, 2013, 2:00 AM), http://www.lasvegassun.com/news/2013/mar/03/its-poker-only-online-gambling-nevada-now/?ixzz2TDTsr3vk.

36. 2013 Nev. Legis. Serv. ch. 2, § 1 (West) (A.B. 114) (to be codified at NEV. REV. STAT. ANN. § 463.6).

37. *Id.*

38. *See* Nev. Gaming Comm'n, Notice of Request for Comments and/or Language on Regulations Concerning Interstate Agreements for Interstate Gaming (Mar. 14, 2013), *available at* http://gaming.nv.gov/modules/showdocument.aspx?documentid=7692.

39. *Id.*

Public comments should guide the NGC in developing rational terms for the interstate compacts with other states. Because comments were solicited from all interested parties, and because comments were offered from in-state, other states, and other countries, the NGC should have a reasonable, preliminary list of negotiating considerations.

C. New Jersey

On February 26, 2013, only days after Nevada took action, the New Jersey Governor signed into law Assembly Bill No. 2578 titled "Authorizes Internet gaming at Atlantic City casinos under certain circumstances."[40] The legislation allows wagering to take place over the internet from certain designated areas within Atlantic City, New Jersey casinos.[41] Like Delaware, it legalizes a full slate of different online games, including internet poker.[42] New Jersey's legislation was the first to allow the state to enter into agreements with foreign countries, as well as domestic interstate compacts.[43] This has triggered further excitement in international gaming venues interested in taking part in the rising tide of internet gambling in the United States.

Problems with Internet Gambling on Indian Lands

The expansion of online poker in the United States would seemingly include the federally recognized Indian tribes that have a strong foothold in brick-and-mortar gambling on Indian reservations. In 2011, the tribes earned an estimated 43.5 percent of casino gaming revenue in the United States.[44] The tribes, however, face uncertainty with respect to internet gambling, specifically because the internet involves off-reservation components that interfere with the tribes' ability to comply with federal law and control their own operations.

First, UIGEA's approach to unlawful internet gambling defers to other laws applicable to any tribe involved in the gambling activity. Thus, gambling will not be unlawful when it is made exclusively within the lands of a single tribe or between the lands of two or more tribes to the extent that inter-tribal gaming is authorized by the Indian Gaming Regulatory Act ("IGRA")[45] or is otherwise

40. 2013 N.J. Sess. Law Serv. ch. 27 (West) (A.B. 2578) (to be codified in scattered subsections of N.J. Stat. Ann. § 5:12).

41. *See id*. § 8 (to be codified at N.J. Stat. Ann. § 5:12-129.12(a)) ("No Internet wagering . . . may be conducted . . . until a casino licensee with a valid operation certificate receives from the division a permit to conduct Internet wagering.").

42. *See id*. § 1 (to be codified at N.J. Stat. Ann. § 5:12-5) ("poker . . . and any above listed game . . . to be offered through Internet wagering"); Ryan Hutchins, *N.J. Moving at Dizzying Pace to Implement Online Gambling* (Mar. 3, 2013, 12:10 AM), http://www.nj.com/politics/index.ssf/2013/03/nj_moving_at_dizzying_pace_to.html.

43. *See* Hutchins, *supra* note 42.

44. Gale Courey Toensign, *Latest Gaming Industry Report: Indian Gaming Made Small Gains in 2011*, Indian Country Today Media Network (Mar. 26, 2013), http://indiancountrytodaymedianetwork.com/2013/03/26/latest-gaming-industry-report-indian-gaming-made-small-gains-2011-148353.

45. 25 U.S.C. §§ 2701–2721 (2012).

authorized, such as by a tribal-state compact.[46] Moreover, the applicable tribal ordinance, resolution, or tribal-state compact must include (1) age- and location-verification requirements reasonably designed to block access to minors and persons located beyond tribal lands and (2) appropriate data security standards to prevent unauthorized access by any person whose age and current location has not been verified accordingly.[47] Further, the bet or wager must not violate any of (1) the Interstate Horseracing Act of 1978,[48] (2) the Professional Amateur Sports Protection Act,[49] (3) the Gambling Devices Transportation Act,[50] or (4) IGRA.[51]

UIGEA essentially provides a safe harbor for transactions that meet certain conditions and do not violate other applicable laws.[52] However, the determination of whether one benefits from the safe harbor is no mean feat. The reference to, and allowance of, intra-tribal and inter-tribal transactions impliedly excludes off-reservation transactions based on the principle of *expressio unius est exclusio alterius*, i.e., the expression of one thing means the exclusion of another.[53] The UIGEA safe harbor references "Indian lands," as defined in IGRA.[54] IGRA defines the term "Indian lands" as "(A) all lands within the limits of any Indian reservation; and (B) any lands title to which is either held in trust by the United States for the benefit of any Indian tribe or individual or held by any Indian tribe or individual subject to restriction by the United States against alienation and over which an Indian tribe exercises governmental power."[55] The Office of General Counsel of the National Indian Gaming Commission ("NIGC") advised that the "use of the Internet, even though the computer server may be located on Indian lands, would constitute off-reservation gaming to the extent any of the players were located off of Indian lands."[56] Consequently, a tribal internet gambling site would violate UIGEA if there were any off-reservation bettors or other off-reservation components, converting otherwise "lawful Internet gambling" into "unlawful Internet gambling."[57]

Even if the interpretation of UIGEA were not problematic, the possible, if not likely, classification of internet poker as Class III gaming would hinder any tribe's ability to offer such gaming activities unless there was a tribal-state

46. 31 U.S.C. § 5362(10)(C)(i)–(ii) (2012).
47. *Id.* § 5362(10)(C)(iii)(I)–(II).
48. 15 U.S.C. §§ 3001–3007 (2012).
49. 28 U.S.C. §§ 3701–3704 (2012).
50. 15 U.S.C. §§ 1171–1178 (2012).
51. 31 U.S.C. § 5362(10)(C)(iv)(I)–(IV) (2012).
52. *Id.* § 5362(10)(C).
53. Black's Law Dictionary 581 (6th ed. 1990).
54. 31 U.S.C. § 5362(10)(C)(i) (2012); *see also* Memorandum on the Applicability of 25 U.S.C. § 2719 to Restricted Fee Lands from David Longly Bernhardt, Solicitor, Dep't of Interior, to Sec'y. of Interior 1–7 (Jan. 18, 2009), *available at* http://www.doi.gov/solicitor/opinions/M-37023.pdf.
55. 25 U.S.C. § 2703(4) (2012); *see also* 25 C.F.R. § 502.12 (2013).
56. Letter from Kevin K. Washburn, Gen. Counsel, Nat'l Indian Gaming Comm'n, to Joseph M. Speck, Nic-A-Bob Prods. (Mar. 13, 2001), *available at* http://www.nigc.gov/Reading_Room/Game_Classification_Opinions-old/Class_III_Games/Class_III_Game-16.aspx.
57. 31 U.S.C. § 5363 (2012) (generally prohibiting the business of "unlawful Internet gambling").

compact.[58] It is not clear at present whether poker games offered over the internet are Class II or Class III gaming. The determination could vary depending on the specifics of the internet poker game in question. IGRA grants tribes the exclusive right to regulate Class II gaming, subject to supervision of the NIGC, if the gaming activity is not prohibited under federal law or by the state in which the tribe is located.[59] Class II includes bingo (whether or not "technologic aids" are used) and non-banking card games, but does not include "electronic or electromechanical facsimiles of any game of chance or slot machines of any kind."[60] Class III is a catch-all classification that includes all gaming other than Class I or Class II gaming,[61] and for the most part consists of casino-type games. In order for a tribe to engage in legal Class III gaming, the tribe has to have a gaming compact with the state.[62]

In a December 2009 memorandum opinion by the NIGC, the commission explored the differences between a "technologic aid" and an "electronic or electromechanical facsimile" for purposes of defining the scope of Class II gaming, which indirectly shed significant light on the scope of legal internet gambling on tribal lands.[63] In simple terms, if something in the nature of an electronic component merely assists the players, it is merely a "technologic aid," and if it is an all-encompassing alternate way to play the game, it is an "electronic or electromechanical facsimile."[64] Using that simple explanation as a guide, it would appear that an internet poker game that incorporates all aspects of the game to be played entirely over the internet at an off-reservation location would likely be classified as Class III gaming. Because internet poker likely would be classified as Class III gaming, it could only be legally offered pursuant to a state compact.[65] Many battles lie ahead over that general issue and possibly a myriad of poker configurations involving technological aids to avoid Class III classification.[66]

Globalization of U.S. Internet Gambling

Internet gambling is not new to much of the rest of the world, but the expanding market in the United States is new and the tribes are not likely to be left on the sidelines. In April 2013, the State of Oklahoma and the Cheyenne and

58. 25 U.S.C. § 2710(d)(1) (2012).
59. *See id.* §§ 2701(5), 2710(a)(2).
60. *Id.* § 2703(7).
61. *Id.* § 2703(8); *compare id.* § 2703(6) (defining "class I gaming" to mean social games for prizes of minimal value or traditional ceremonial games).
62. *Id.* § 2710(d)(1)(C).
63. Memorandum on the Classification of Card Games Played with Technologic Aid from Penny J. Coleman, Acting Gen. Counsel, Nat'l Indian Gaming Comm'n, to George T. Skibine, Acting Chairman, Nat'l Indian Gaming Comm'n (Dec. 17, 2009), *available at* http://www.nigc.gov/Portals/0/NIGCUploads/readingroom/gameopinions/Cardgamesplayedwithtechaids121709.pdf.
64. *See id.* at 1–11.
65. 25 U.S.C. § 2710(d)(1).
66. Norm DesRosiers, *Internet Poker: Is It Class II Gaming?*, Casino Ent. Mgmt. (Aug. 31, 2012), http://www.casinoenterprisemanagement.com/articles/september-2012/internet-poker-it-class-ii-gaming.

Arapaho Tribes entered into a Class III gaming compact to share revenues from international gaming, while banning in-state internet gambling in the State of Oklahoma.[67] This appears to be the first Class III state compact entered into between a state and a tribe related to international internet gambling, and may indeed be those tribes' way of getting the jump on and competing with state-foreign international compacts that are sure to follow.

Although it may not be connected to U.S. expansion, interest in internet gambling is also picking up in new international venues. By way of example, on March 27, 2013, the Romanian government passed an emergency ordinance establishing a new authority—the National Gambling Office ("NGO")—for the regulation of gambling.[68] The NGO will regulate online gambling activities operating within Romania and remotely provided services to Romania.[69]

These expansionist activities by unlikely parties may be another tell-tale sign that internet gambling is in high gear and going global like never before.

67. Patrick B. McGuigan, *OK Gov. Fallin Signs Trio of Agreements with Cheyenne & Arapaho Tribes*, OKLA. WATCHDOG (Apr. 6, 2013), http://watchdog.org/78472/ok-gov-fallin-signs-trio-of-agreements-with-cheyenne-arapaho-tribes/.

68. Gemma Boore, Moris Mashali & Michael McCormack, *Could This Be the Beginning of a Global Market of Regulated Gambling Jurisdictions?*, MARTINDALE (Apr. 9, 2013), http://www.martindale.com/internet-law/article_Edwards-Wildman-Palmer-LLP_1748366.htm.

69. *Id.*

Recent Developments in Cyberspace Law: A View from Brazil

*By Renato Opice Blum and Rita P. Ferreira Blum**

Introduction

As in other Latin American countries, internet usage and e-commerce transactions are growing rapidly in Brazil. According to a 2011 survey, the percentage of internet users making online purchases had increased by 10 percent over 2010.[1] A Brazilian report states that the total nominal amount of e-commerce sales had increased by 26 percent from 2010 to 2011, generating total revenue of 18.7 billion reais.[2]

In recognition of an expanded role for the internet in our society, the Brazilian legislature has recently enacted new rules affecting transactions in cyberspace. Courts have also issued some key decisions interpreting existing laws in the cyberspace domain. These developments are discussed below as they relate to three critical areas: the protection of consumers in the internet environs, protection of personality rights, and protection of businesses and consumers from unauthorized computer access.

I. Consumer Protection Rules

Consumer protection in Brazil is mainly regulated by Federal Law No. 8,078 of 1990, the Consumer Protection Code.[3] In Brazil, the concept of *consumer* is not limited to an individual, as it includes any legal entity that acquires or uses a good or a service in the capacity of an end-user if that good or service was provided by a *supplier*.[4] A *supplier* includes any individual or legal entity that

* Renato Opice Blum is a partner at Opice Blum, Bruno, Abrusio and Vainzof Attorneys at Law. He is President of the American Chamber of Commerce Technology Law Committee and Vice President of the Brazilian Bar Electronic Law and High Technology Crimes Commission. Rita P. Ferreira Blum is a senior associated lawyer at the firm and author of the book *Consumer Rights on the Internet*.

1. *See* Brazilian Internet Steering Comm., ICT Households and Enterprises 2011: Survey on the Use of Information and Communication Technologies in Brazil (2012), *available at* http://op.ceptro.br/cgi-bin/cetic/tic-domicilios-e-empresas-2011.pdf (a publication of "cetic.br").

2. *See* WebShoppers Report 11 (25th ed. 2012), *available at* http://institucional.geravd.com.br/arquivos/acontece/WebShoppers.pdf.

3. "Código de Proteção e Defesa do Consumidor—(C.D.C)." The law is Lei No. 8.078, de 11 de Setembro de 1990, Diário Oficial da União—Supp. [D.O.U.] de 12.09.1990 (Braz.)

4. *See id.* art. 2. Thus, even corporations may fit the definition of consumer for purposes of the C.D.C.

carries on a professional business and offers products for sale or renders services to *consumers*.[5]

Consumers in Brazil enjoy a *right of retraction* ("direito de arrependimento") that applies whenever goods or services are acquired outside of a commercial establishment, especially through the telephone or at an individual's domicile.[6] Article 49 of the Consumer Protection Code provides consumers with the right to retract within seven days of the point of contract or of the date the good or service is received.[7] Should the consumer exercise this right, the supplier must return any consideration made in full.[8]

Article 31 of Consumer Protection Code establishes that suppliers of services or products must provide consumers with clear, accurate, and accessible information in Portuguese about the products or services they purchase.[9] This includes such matters as the product characteristics, price, warranty, and origin, as well as any risks presented to consumer health and safety.[10]

Brazilian Decree No. 7,962, which is effective beginning May 14, 2013, clarifies that these consumer protection requirements from Articles 49 and 31 also apply to e-commerce transactions.[11] Main aspects of the decree include a requirement to disclose such terms as freight, cost of the insurance (if applicable), and the deadline for delivery of the goods or performance of the service.[12] Websites are also required to show the supplier's data (i.e., company name; Brazilian taxpayer's Registry Number, if it exists, as well as the address of the company's business premises and its e-mail address).[13] The Decree also

5. As per article 3d of the C.D.C., "Supplier is any public or private, national or foreign individual or body corporate, as well as entities without a legal identity carrying on business in the field of production, assembly, creation, construction, transformation, import, export, distribution or commercialization of products, or rendering of services." *Id.* art. 3.

6. As per art. 49 of the C.D.C., "The consumer may give up a contract within a period of seven days from its signature or reception of the good or service, whenever contracting products and services outside of a commercial establishment, especially through the telephone or at his domicile." *Id.* art. 49.

7. *See id.*

8. As per art. 49 of the C.D.C., sole paragraph, "If the consumer exercises the right of retraction as mentioned in this article, the amount possibly paid in advance for any reason during this period of consideration shall be returned promptly with the corresponding adjustments." *Id.*

9. As per art. 31 of the C.D.C., "The offer and presentation of products or services shall ensure correct, clear, accurate, and accessible information in Portuguese on their characteristics, quality, quantity, components, price, warranty, duration and origin, among other data, as well as about the risks they might involve to consumers' health and safety." *Id.* art. 31.

10. *See id.*

11. Decreto No. 7.962, de 15 de Março de 2013, Diário Oficial da União [D.O.U.], Edição Extra, de 15.03.2013.

12. As per art. 2d, items IV and V of Decree No. 7,962/13: "The websites or other electronic ways used to offer or conclude a contract with the consumer shall provide, in a prominent place where it is easily visible, the following information: (. . .) IV—distinguish the price of any additional expenses, such as freight or insurance; V—full terms of the offer, including methods of payment, availability of the service or product, manner and time in which the service will be performed or the product will be delivered to the consumer." *Id.* art. 2.

13. As per art. 2d, items I and II of Decree No. 7,962/13: "The websites or other electronic ways used to offer or conclude a contract with the consumer shall provide, in a prominent place where it is easily visible, the following information: I—trade name and Brazilian taxpayer's Registry Number, when applicable, either in case of an individual who acts as a supplier, or in case of a legal entity

addresses required notice of the consumer's right of retraction in the online environment.[14]

II. Right to Protect Personality Rights in the Online Environment

The right to protect one's honor and image in the online environment has also been recently addressed. Personality rights in Brazil (i.e., those governing one's personal honor, image, and other personal rights) are governed by a set of legal instruments, including the Brazilian Federal Constitution of 1988, the Brazilian Civil Code (Federal Law No. 10,406/2002),[15] and the Brazilian Criminal Code (Law Decree No. 2,848/1940),[16] which need to be constructed and reviewed jointly in order to understand fully their implications.

Personality rights are directly connected to the dignity of the human person, which is a fundamental right of the Brazilian Republic under the Federal Constitution of 1988.[17] Civil liability is mainly regulated by the Brazilian Civil Code, which basically provides a basis for redress whenever an individual or legal entity causes damage or violates the rights of an another individual or legal entity on account of an act or voluntary omission done negligently or recklessly.[18] Finally, the Penal Code also sanctions individual voluntary conduct against the honor and reputation of another individual, which includes slander, defamation, and libel.[19]

A recent case illustrates the application of these personality rights in the context of a take-down request of an internet service provider, which was a novel question in Brazil. In a civil case involving a claim against a social media site originally brought by *Mrs. Graziele Salme Leal* against *Google Brasil Internet Ltda.*, Brazil's highest court of appeals on all non-constitutional matters announced that a twenty-four hour deadline would be imposed on an internet service provider to remove content or an image that an individual claims may constitute an offense to her honor (i.e., personality rights).[20] Failure to comply could result in civil liability for any harm to the claimant.[21] Significantly, the court required removal as

that acts as a supplier; II—physical and electronic addresses, and other data for contact and for identification of the supplier." *Id.*

14. As per art. 5th of Decree No. 7,962/13: "The supplier shall inform in a clear and noticeable manner, the appropriate and effective ways for the consumer to exercise the right of retraction." *Id.* art. 5.

15. Lei No. 10.406, de 10 de Janeiro de 2002, Diário Oficial da União [D.O.U.] de 11.01.2002 (Braz.). The name of this Code in Portuguese is "Código Civil—C.C."

16. Decreto-Lei No. 2.848, de 07 de Dezembro de 1940, Diário Oficial da União [D.O.U.] de 31 de Dezembro de 1940 (Braz.). The name of this Code in Portuguese is "Código Penal—C.P."

17. *See* art. 1st, item III, and art. 5th, item X of the Constitution ("Constituição Federal—C.F.").

18. *See* articles 20, 186, 187, and 189 of the Civil Code ("Código Civil—C.C."), *cited in supra* note 15.

19. *See* articles 138 (slander), 139 (defamation), and 140 (libel) of the Penal Code ("Código Penal—C.P."), *cited in supra* note 16.

20. Superior Tribunal de Justiça (S.T.J.) REsp No. 1323754-RJ (2012/0005748-4), Relator: Min. Nancy Andrighi, 19.06.2012, *available at* http://goo.gl/pzk0bz.

21. *See* item 2 of the summary of the S.T.J.'s decision *cited in supra* note 20 and also page 6 of the decision.

a preventive or protective matter, but allowed a later determination to ascertain whether the claim being asserted was accurate, after which the site may republish the information if personal rights are not being implicated.[22] The case is notable because no specific Brazilian law regulates the required response to a take-down request. Thus, the matter is being regulated entirely through judge-made law rooted in interpreting constitutional and statutory rights.

In this context, it is interesting to compare the U.S. and the Brazilian legal systems. Whereas in the U.S. legal system "notice and take down" is frequently connected with user-generated content that infringes copyright or other intellectual property rights, in Brazil the "notice and take down" expression is being used in a colloquial manner (i.e., "*lato sensu*") to refer primarily to the act of requesting that an internet service provider remove offending content that violates personality rights, whether generated by a provider or another web-user.

III. Criminal Laws Affecting Unauthorized Computer Access

Rising levels of computer crime have also affected Brazilian business firms, which helps explain a new criminal law affecting unauthorized computer access. Enacted in December 2012, Federal Law No. 12,737/2012[23] addresses important issues such as: (i) hacking of electronic devices, (ii) unauthorized remote invasive conduct in violation of security measures of the victim, and (iii) interruption of telematic services. Although Federal Law No. 12,737/2012 is an important symbolic step that signals greater legal significance for the value of data and information, the practical impact on doing business in Brazil is difficult to perceive. For example, the law imposes criminal sanctions on unauthorized access and use of private information, but the penalties imposed for violations appear quite modest considering that sensitive business information of an incalculable value could be affected.[24] Thus, among other things, it is unclear whether the criminal penalties applied for violations of these provisions will create an adequate deterrent effect for those inclined to unlawful access.

Nevertheless, Federal Law No. 12,737/2012 is significant because it adds to the Brazilian legal system, for the first time, criminal penalties for unauthorized computer access. As such, it reinforces social and private companies' expectation of privacy and security in cyberspace, and thus may set the stage for further legal protections in this area.

22. *See* item 3 of the summary of the S.T.J.'s decision *cited in supra* note 20 and also page 6 of the decision.

23. Lei No. 12.737, de 30 de Novembro de 2012, Diário Oficial da União [D.O.U.] de 03.12.2012 (Braz.).

24. *See* articles 2d and 3d for information about penalties of the conduct typified in Lei No. 12.737, de 30 de Novembro de 2012, *cited in supra* note 23. An aggrieved company might also file a civil lawsuit for monetary damages, which provides additional deterrent effects apart from criminal sanctions. For more details about civil liability in Brazil, see articles 186, 187, 189, and 927 of the Civil Code ("Código Civil–C.C."), *cited in supra* note 15.

IV. Conclusion

Brazilian laws governing cyberspace are progressing toward solutions for some of the important problems affecting consumers and businesses in this domain. These developments may be precursors to the construction of a major Brazilian legislation framework on this subject, but in the meantime they help attend to social expectations for more security in cyberspace, including greater protections for both commercial and personal rights.